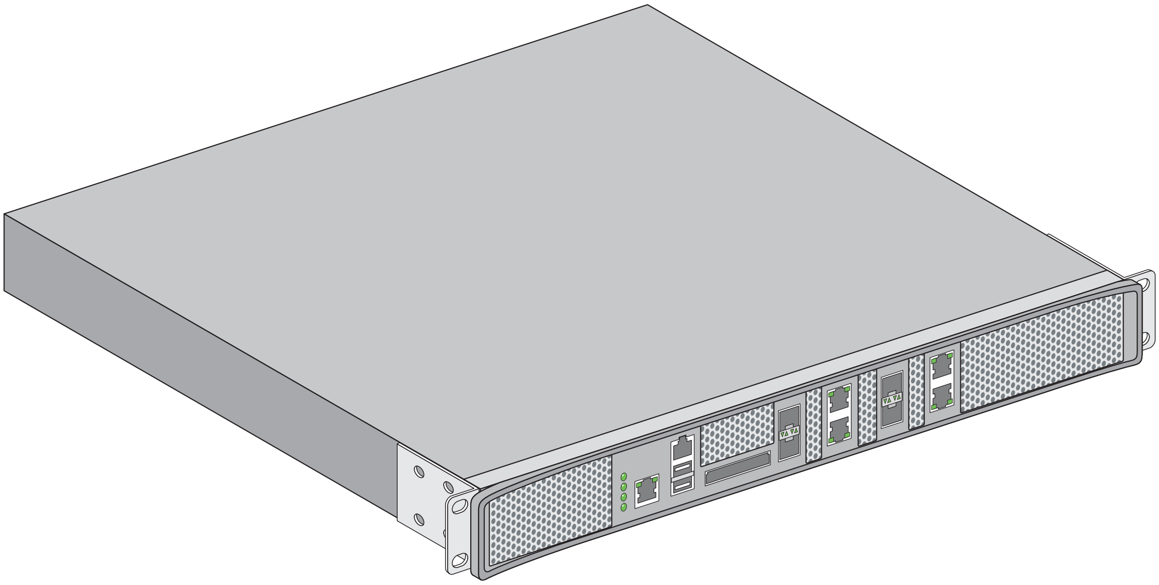
MOTOROLA

RFS7000 Series RF Switch

CLI Reference Guide



About This Guide

This preface introduces the *RFS7000 Series CLI Reference Guide* and contains the following sections:

- *Who Should Use this Guide*
- *How to Use this Guide*
- *Conventions Used in this Guide*
- *Motorola Service Information*

Who Should Use this Guide

The *RFS7000 Series CLI Reference Guide* is intended for system administrators responsible for the implementing, configuring, and maintaining the RFS7000 using the switch *command line interface* (CLI). It also serves as a reference for configuring and modifying most common system settings. The administrator must be familiar with wireless technologies, network concepts, ethernet concepts, as well as IP addressing and SNMP concepts.

How to Use this Guide

This guide helps you implement, configure, and administer the RFS7000 Switch and associated network elements. This guide is organized into the following sections:

Table 1 Quick Reference on How This Guide Is Organized

Chapter	Jump to this section if you want to...
Chapter 1, “Introduction”	Review the overall feature-set of the RFS7000 Switch, as well as the many configuration options available.
Chapter 2, “Common Commands”	Summarizes the commands common amongst many contexts and instance contexts within the RFS7000 Switch CLI.
Chapter 3, “User Exec Commands”	Summarizes the User Exec commands within the RFS7000 Switch CLI.
Chapter 4, “Privileged Exec Commands”	Summarizes the Priv Exec commands within the RFS7000 Switch CLI.
Chapter 5, “Global Configuration Commands”	Summarizes the Global Config commands within the RFS7000 Switch CLI.
Chapter 6, “crypto-trustpoint Instance”	Summarizes the **`(crypto-trustpoint)`** commands within the RFS7000 Switch CLI.
Chapter 7, “interface Instance”	Summarizes the **`(config-if)`** commands within the RFS7000 Switch CLI.
Chapter 8, “spanning tree-mst Instance”	Summarizes the **`(config-mst)`** commands within the RFS7000 Switch CLI.

Table 1 Quick Reference on How This Guide Is Organized (Continued)

Chapter	Jump to this section if you want to...
Chapter 9, “Extended ACL Instance”	Summarizes the **(config-ext-nacl)** commands within the RFS7000 Switch CLI.
Chapter 10, “Standard ACL Instance”	Summarizes the **(config-std-nacl)** commands within the RFS7000 Switch CLI.
Chapter 11, “Extended MAC ACL Instance”	Summarizes the **(config-ext-macl)** commands within the RFS7000 Switch CLI.
Chapter 12, “DHCP Instance”	Summarizes the **(config-dhcp pool)** commands within the RFS7000 Switch CLI.
Chapter 13, “RADIUS Server Instance”	Summarizes the **(config-radsrv)**instance commands within the RFS7000 Switch CLI.
Chapter 14, “Wireless Instance”	Summarizes the **(config-wireless)**instance commands within the RFS7000 Switch CLI.

Conventions Used in this Guide

This section describes the following topics:

- *Annotated Symbols*
- *Notational Conventions*

Annotated Symbols

The following document conventions are used in this document:

NOTE Indicates tips or special requirements.

CAUTION Indicates conditions that can cause equipment damage or data loss.

WARNING! Indicates a condition or procedure that could result in personal injury or equipment damage.

Notational Conventions

The following notational conventions are used in this document:

- Italics are used to highlight specific items in the general text, and to identify chapters and sections in this and related documents.
- Bullets (•) indicate:
  - action items
  - lists of alternatives
  - lists of required steps that are not necessarily sequential
- Sequential lists (those describing step-by-step procedures) appear as numbered lists.

Table 1-1. Notational Convention used in the document

Convention	***Example Token***	***Description***	***Valid Inputs***
bold		Bold text indicates commands and keywords that you enter literally	
italics		Italic text indicates arguments for which you supply values.	
()	(on|off)	Grouping (exactly one of a list of tokens)	on
{}	{key1|key2|key3}	Selective recursive (multiple tokens allowed, but each can only be used once)	key1 key3
[ ]	[key1|key2|key3]	Infinite recursive (multiple tokens allowed, each can be used multiple times)	key1 key1 key2 key3 key2 key3
.	.<1-10>	Simple infinite recursive	1 2 6
?	[key1|?key2]	Selective keyword in infinite recursive.	key1 key1 key2

Motorola Service Information

Use the Motorola Support Center as the primary contact for any technical problem, question, or support issue involving Motorola products. Motorola Support Center responds to calls by email, telephone or fax within the time limits set forth in individual contractual agreements:

Telephone (North America): 1-800-653-5350
Telephone (International): +1-631-738-6213
Fax: (631) 738-5410
Email: http://www.symbol.com/support/

When contacting Motorola Support Center, please provide the following information:

- Serial number of the unit.
- Model number or product name.
- Software type and version number.

Customer Support Website

Comprehensive on-line support is available at the MySymbolCare Web site at http://www.symbol.com/support/ . Registration is free and a variety of services can be linked through this Web portal.

Product Sales and Product Information

North America	***International***
Motorola, Inc. One Symbol Plaza Holtsville, New York 11742-1300 Tel: 1-631-738-2400 or 1-800-722-6234 Fax: 1-631-738-5990	Motorola, Inc. Symbol Place Winnersh Triangle, Berkshire, RG41 5TP United Kingdom Tel: 0800-328-2424 (Inside UK) +44 118 945 7529 (Outside UK)

General Information

For general information, contact Motorola at:

Telephone (North America): 1-800-722-6234
Telephone (International): +1-631-738-5200
Website: http://www.motorola.com

Motorola, Inc.
End-User License Agreement

BY DOWNLOADING, INSTALLING, OR USING THE SOFTWARE DESCRIBED IN THIS DOCUMENT, YOU OR THE ENTITY OR COMPANY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THIS LICENSE AGREEMENT ("AGREEMENT"). LICENSEE'S USE OR CONTINUED USE OF THE DOWNLOADED OR INSTALLED MATERIALS SHALL ALSO CONSTITUTE ASSENT TO THE TERMS OF THIS AGREEMENT. IF LICENSEE DOES NOT UNCONDITIONALLY AGREE TO ALL OF THE TERMS OF THIS AGREEMENT, DO NOT CONTINUTE THE INSTALLATION PROCESS. IF THESE TERMS ARE CONSIDERED AN OFFER, ACCEPTANCE IS EXPRESSLY LIMITED TO AND EXPRESSLY CONTINGENT UPON THESE TERMS. IF YOU ARE ACCEPTING THESE TERMS ON BEHALF OF A COMPANY, ANOTHER PERSON OR ANY OTHER LEGAL ENTITY, YOU REPRESENT AND WARRANT THAT YOU HAVE THE AUTHORITY TO BIND THAT COMPANY, PERSON OR ENTITY.

1. LICENSE GRANT. Subject to the terms of this Agreement, Motorola, Inc. and/or its subsidiaries ("Licensor") hereby grants Licensee a limited, personal, non-sublicensable, non transferable, nonexclusive license to use the software that Licensee is about to download or install and the documentation that accompanies it (collectively, the "Software") for Licensee's personal use in connection with hardware produced by Licensor and only in accordance with the accompanying documentation. Licensee may download, install and use the Software only on a single computer. Licensee may make one copy of the Software (excluding any documentation) for backup purposes, provided that copyright and other restricted rights notices of Licensor and its suppliers are reproduced exactly.
2. LICENSE RESTRICTIONS. Except as expressly permitted by this Agreement, Licensee shall not, nor permit anyone else to, directly or indirectly: (i) copy (except for one backup copy), modify, distribute or create derivative works based upon the Software; (ii) reverse engineer, disassemble, decompile or otherwise attempt to discover the source code or structure, sequence and organization of the Software; or (iii) rent, lease, or use the Software for timesharing or service bureau purposes, or otherwise use the Software for any commercial purpose/on behalf of any third party. Licensee shall maintain and not remove or obscure any proprietary notices on the Software, and shall reproduce such notices exactly on all permitted copies of the Software. All title, ownership rights, and intellectual property rights in and to the Software, and any copies or portions thereof, shall remain in Licensor and its suppliers or licensors. Licensee understands that Licensor may modify or discontinue offering the Software at any time. The Software is protected by the copyright laws of the United States and international copyright treaties. The Software is licensed, not sold. This Agreement does not give Licensee any rights not expressly granted herein.
3. INTELLECTUAL PROPERTY; CONTENT. All title and intellectual property rights in and to the Software (including but not limited to any images, photographs, animations, video, audio, music, text and "applets" incorporated into the Software), and any copies you are permitted to make herein are owned by Licensor or its suppliers. All title and intellectual property rights in and to the content which may be accessed through use of the Software is the property of the respective content owner and may be protected by applicable copyright or other intellectual property laws and treaties. This EULA grants you no rights to use such content. As a condition to Licensee's use of the Software, Licensee represents, warrants and covenants that Licensee will not use the Software: (i) to infringe the intellectual property rights or proprietary rights, or rights of publicity or privacy, of any third party; (ii) to violate any applicable law, statute, ordinance or regulation; (iii) to disseminate information or materials in any form or format ("Content") that are harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, or otherwise objectionable; or (iv) to disseminate any software viruses or any other computer code, files or programs that mayinterrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment. Licensee, not Licensor, remains solely responsible for all Content that Licensee uploads, posts, e-mails, transmits, or otherwise disseminates using, or in connection with, the Software.
4. FEES; SUPPORT AND UPGRADES. Licensor may, at Licensor's sole option, provide support services related to the Software ("Support Services"). Nothing in this Agreement grants Licensee any right to receive any Support Services. Use of any Support Services provided is governed by the Licensor policies and programs described in the user manual, in "online" documentation, and/or in other Licensor-provided materials or support agreements. Any supplemental software code provided to you as part of any Support Services shall be considered part of the Software and subject to the terms and

conditions of this EULA. With respect to technical information you provide to Licensor as part of any Support Services, Licensor may use such information for its business purposes, including for product support and development. Licensor will not utilize such technical information in a form that personally identifies Licensee.

5. TERMINATION. Either party may terminate this Agreement at any time, with or without cause, upon written notice. Any termination of this Agreement shall also terminate the licenses granted hereunder. Upon termination of this Agreement for any reason, Licensee shall return all copies of the Software to Licensor, or destroy and remove from all computers, hard drives, networks, and other storage media all copies of the Software, and shall so certify to Licensor that such actions have occurred. Sections 2-13 shall survive termination of this Agreement.
6. DISCLAIMER OF WARRANTIES. To the maximum extent permitted by applicable law, Licensor and its suppliers provide the Software and any (if any) Support Services AS IS AND WITH ALL FAULTS, and hereby disclaim all warranties and conditions, either express, implied or statutory, including, but not limited to, any (if any) implied warranties or conditions of merchantability, of fitness for a particular purpose, of lack of viruses, of accuracy or completeness of responses, of results, and of lack of negligence or lack of workmanlike effort, all with regard to the Software, and the provision of or failure to provide Support Services. ALSO, THERE IS NO WARRANTY OR CONDITION OF TITLE, QUIET ENJOYMENT, QUIET POSSESSION, CORRESPONDENCE TO DESCRIPTION, OR NONINFRINGEMENT WITH REGARD TO THE SOFTWARE. THE ENTIRE RISK AS TO THE QUALITY OF OR ARISING OUT OF USE OR PERFORMANCE OF THE SOFTWARE AND SUPPORT SERVICES, IF ANY, REMAINS WITH LICENSEE.
7. EXCLUSION OF INCIDENTAL, CONSEQUENTIAL AND CERTAIN OTHER DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL LICENSOR OR ITS SUPPLIERS BE LIABLE FOR ANY GENERAL, SPECIAL, INCIDENTAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS OR CONFIDENTIAL OR OTHER INFORMATION, FOR BUSINESS INTERRUPTION, FOR PERSONAL INJURY, FOR LOSS OF PRIVACY, FOR FAILURE TO MEET ANY DUTY INCLUDING OF GOOD FAITH OR OF REASONABLE CARE, FOR NEGLIGENCE, AND FOR ANY OTHER PECUNIARY OR OTHER LOSS WHATSOEVER) ARISING OUT OF OR IN ANY WAY RELATED TO THE USE OF OR INABILITY TO USE THE SOFTWARE, THE PROVISION OF OR FAILURE TO PROVIDE SUPPORT SERVICES, OR OTHERWISE UNDER OR IN CONNECTION WITH ANY PROVISION OF THIS AGREEMENT, EVEN IN THE EVENT OF THE FAULT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, BREACH OF CONTRACT OR BREACH OF WARRANTY OF LICENSOR OR ANY SUPPLIER, AND EVEN IF LICENSOR OR ANY SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.
8. LIMITATION OF LIABILITY AND REMEDIES. Notwithstanding any damages that Licensee might incur for any reason whatsoever (including, without limitation, all damages referenced above and all direct or general damages), the entire liability of Licensor and any of its suppliers under any provision of this Agreement and Licensee's exclusive remedy for all of the foregoing shall be limited to the greater of the amount actually paid by Licensee for the Software or U.S.$5.00. The foregoing limitations, exclusions and disclaimers shall apply to the maximum extent permitted by applicable law, even if any remedy fails its essential purpose.

9. INDEMNITY. Licensee agrees that Licensor shall have no liability whatsoever for any use Licensee makes of the Software. Licensee shall indemnify and hold harmless Licensor from any claims, damages, liabilities, costs and fees (including reasonable attorney fees) arising from Licensee's use of the Software as well as from Licensee's failure to comply with any term of this Agreement.
10. FAULT TOLERANCE. The Software is not fault-tolerant and is not designed, manufactured or intended for use or resale in on-line control equipment in hazardous environments requiring fail-safe performance, such as, but not limited to, the operation of nuclear facilities, aircraft navigation or communication systems, air traffic control, life support machines, or weapons systems, in which the failure of the Software could lead directly or indirectly to death, personal injury, or physical or environmental damage ("High Risk Activities"). Licensor and its suppliers specifically disclaim any express or implied warranty of fitness for High Risk Activities.
11. U.S. GOVERNMENT LICENSE RIGHTS. Software provided to the U.S. Government pursuant to solicitations issued on or after December 1, 1995 is provided with the commercial license rights and restrictions described elsewhere herein. Software provided to the U.S. Government pursuant to solicitations issued prior to December 1, 1995 is provided with "Restricted Rights" as provided for in FAR, 48 CFR 52.227-14 (JUNE 1987) or DFAR, 48 CFR 252.227- 7013 (OCT 1988), as applicable. The "Manufacturer" for purposes of these regulations is Motorola, Inc., One Symbol Plaza, Holtsville, NY 11742.
12. EXPORT RESTRICTIONS. Licensee shall comply with all export laws and restrictions and regulations of the Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control ("OFAC"), or other United States or foreign agency or authority, and Licensee shall not export, or allow the export or re-export of the Software in violation of any such restrictions, laws or regulations. By downloading or using the Software, Licensee agrees to the foregoing and represents and warrants that Licensee is not located in, under the control of, or a national or resident of any restricted country.
13. MISCELLANEOUS. Licensee may not sublicense, assign, or transfer this Agreement, or its rights or obligations hereunder, without the prior written consent of Licensor. Any attempt to otherwise sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is null and void. Licensor may assign this Agreement in its sole discretion. In the event that any of the provisions of this Agreement shall be held by a court or other tribunal of competent jurisdiction to be illegal, invalid or unenforceable, such provisions shall be limited or eliminated to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect. No waiver or modification of this Agreement will be binding upon a party unless made in writing and signed by a duly authorized representative of such party and no failure or delay in enforcing any right will be deemed a waiver. This Agreement shall be governed by the laws of the State of New York without regard to the conflicts of law provisions thereof. The application the United Nations Convention of Contracts for the International Sale of Goods is expressly excluded. Unless waived by Licensor for a particular instance, any action or proceeding arising out of this Agreement must be brought exclusively in the state or federal courts of New York and Licensee hereby consents to the jurisdiction of such courts for any such action or proceeding. This Agreement supersedes all prior discussions and writings and constitutes the entire agreement between the parties with respect to the subject matter hereof. The prevailing party in any action arising out of this Agreement shall be entitled to costs and attorneys' fees.

Contents

About This Guide

Chapter 1. Introduction

Chapter 2. Common Commands

Chapter 3. User Exec Commands

Chapter 4. Privileged Exec Commands

Chapter 5. Global Configuration Commands

Chapter 6. crypto-trustpoint Instance

Chapter 7. interface Instance

Chapter 8. spanning tree-mst Instance

Chapter 9. Extended ACL Instance

Chapter 10. Standard ACL Instance

Chapter 11. Extended MAC ACL Instance

Chapter 12. DHCP Instance

Chapter 13. RADIUS Server Instance

Chapter 14. Wireless Instance

Appendix A Customer Support

1

Introduction

This chapter describes the commands defined by the RFS7000 Series *Command Line Interface* (CLI). Access the CLI by running a terminal emulation program on a computer connected to the serial port at the front of the switch, or by using telnet or secure shell (ssh) to access the switch over the network.

The default cli user is **cli**. The default username and password is admin and superuser, respectively.

1.1 CLI Overview

The CLI is used for configuring, monitoring, and maintaining Motorola devices. The user interface allows you to execute commands, whether using a serial console or using remote access methods.

This chapter describes the basic features of the Motorola CLI and how to use them. Topics covered include an introduction to command modes, navigation and editing features, help features, and command history features.

The CLI is divided into different command modes. Each command mode has its own set of commands available for configuration, maintenance and monitoring. The commands available at any given time depend on the mode you are in. Enter a question mark (**?**) at the system prompt to view the list of commands available for each command mode/instance.

Use specific commands to navigate from one command mode to another. The standard order is as follows: USER EXEC mode; PRIV EXEC mode and GLOBAL CONFIG mode.

A session generally begins in USER EXEC mode, which is one of the two access levels of EXEC mode. For security purposes, only limited subset of EXEC commands are made available in USER EXEC mode. This level of access is reserved for tasks that do not change the configuration of the switch, such as determining the current switch configuration.

To access commands, enter the PRIV EXEC mode, which is the second level of access for the EXEC mode. In the PRIV EXEC mode, enter any EXEC command. The PRIV EXEC mode is a superset of the USER EXEC mode.

Most of the USER EXEC mode commands are one-time commands and are not saved across reboots of the switch. For example, show command displays the current configuration and clear command clears the counter or interface.

Enter GLOBAL CONFIG mode from PRIV EXEC mode. In this mode, enter commands that configure general system characteristics. Use the global configuration mode to enter specific configuration modes. Configuration modes, including global configuration mode, allows you to make changes to the running configuration. If you save the configuration later, these commands are stored across switch reboots.

Enter a variety of protocol-specific or feature-specific configuration modes from global configuration mode. The CLI hierarchy requires you enter these specific configuration modes only through global configuration mode.

Enter configuration submodes from global configuration modes. Configuration submodes are used to configure specific features within the scope of a given configuration mode.

The *Table 1.1* below summarizes the commands available to configure and monitor the switch.

Table 1.1 CLI Context Hierarchy for RFS7000

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
clear	acknowledge	aaa
clrscr	archive	access-list
cluster-cli	cd	autoinstall
debug	change-passwd	banner
disable	clear	boot
enable	clock	bridge
exit	clrscr	clrscr
help	cluster-cli	country-code
logout	configure	crypto
no	copy	debug
page	debug	do
quit	delete	end
service	diff	errdisable
show	dir	exit
terminal	disable	format
write	edit	ftp
	enable	help
	erase	hostname

Table 1.1 CLI Context Hierarchy for RFS7000

User Exec Mode	***Priv Exec Mode***	***Global Configuration Mode***
	exit	interface
	help	ip
	kill	license
	logout	line
	mkdir	logging
	more	mac
	no	management
	page	no
	ping	ntp
	pwd	prompt
	quit	radius-server
	reload	redundancy
	rename	service
	rmdir	show
	service	snmp-server
	show	spanning-tree
	telnet	timezone
	terminal	username
	traceroute	vlan
	upgrade	wireless
	upgrade-abort	wlan-acl
	write	

1.2 Getting Context Sensitive Help

Enter a question mark (**?**) at the system prompt to display a list of commands available for each command mode. You also can optionally obtain a list of the arguments and keywords available for any command using context-sensitive help.

Use any of the following commands to get help specific to a command mode, command name, keyword or argument:

Command	***Description***
(prompt)# **help**	Displays a brief description of the help system.
(prompt)# abbreviated-command-entry **?**	Lists commands in the current mode that begin with a particular character string.
(prompt)# abbreviated-command-entry **<Tab>**	Completes a partial command name.
(prompt)# **?**	Lists all commands available in the command mode.
prompt)# command ?	Lists the available syntax options (arguments and keywords) for the command.
(prompt)# command keyword ?	Lists the next available syntax option for the command.

NOTE The system prompt ma varies depending on which configuration mode you are in.

When using context-sensitive help, the space (or lack of a space) before the question mark (?) is significant. To obtain a list of commands that begin with a particular character sequence, type in those characters followed immediately by the question mark (?). Do not include a space. This form of help is called **word help**, because it completes a word.

```
RFS7000#service?
  service  Service Commands

RFS7000#service
```

Enter a question mark (?) in place of a keyword or argument to list keywords or arguments. Include a space before the **?**. This form of help is called **command syntax help** and it shows which keywords or arguments are available based on the command/ keywords and arguments already entered.

```
RFS7000>service ?
  diag      Diagnostics
  encrypt   Encrypt password or key with secret
  locator   flash all LEDS to locate switch visually
  save-cli  Save CLI tree for all modes in html format
  show      Show running system information

RFS7000>service
```

It is possible to abbreviate commands and keywords to the number of characters allowing a unique abbreviation. For example, configure terminal can be abbreviated as `config t`. Since the abbreviated form of the command is unique, the switch accepts the abbreviated form and executes the command.

Enter the help command (available in any command mode) to provide the following description of the help system:

```
RFS7000>help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
```

```
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000>
```

1.3 Using the no and default forms of Commands

Almost every configuration command has a `no` form. In general, use the no form to disable a feature or function. Use the command without the no keyword to re enable a disabled feature or enable a feature disabled by default.

1.4 Basic Conventions

The following are conventions to keep in mind while working within the CLI:

- Always use **?** at the end of the command to view if there are any further sub modes that can be used. If so, type the first few alphabets of the submode and press the tab key. Continue using **?** until you reach the final sub-submode.
- Pre-defined CLI commands and keywords are case-insensitive: `cfg = Cfg = CFG`. For clarity, CLI commands and keywords are displayed using mixed case. For example, `apPolicy`, `trapHosts`, `channelInfo`.
- Commands can be entered in uppercase, lowercase, or mixed case. Only passwords are case sensitive.
- If an instance name (or other parameter) contains a whitespace, the name must be enclosed in quotes:

```
RFS7000.(Cfg)> spol "Default Switch Policy"
RFS7000.(Cfg).SPolicy.[Default Switch Policy]>
```

NOTE CLI commands starting with `#`, at the `RFS7000#` prompt, is ignored and is not executed.
Any leading space before a CLI command is ignored in execution

1.5 Using CLI Editing Features and Shortcuts

A variety of shortcuts and editing features are enabled for the CLI. The following sections describe these features:

- *Moving the Cursor on the Command Line*
- *Completing a Partial Command Name*
- *Deleting Entries*
- *Re-displaying the Current Command Line*
- *Transposing Mistyped Characters*
- *Controlling Capitalization*

1.5.1 Moving the Cursor on the Command Line

Table 1.2 shows the key combinations or sequences to move the cursor on the command line to make corrections or changes. **Ctrl** indicates the Control key, which must be pressed simultaneously with its associated letter key. **Esc** indicates the Escape key, which must be pressed first, followed by its associated letter key. Keys are not case sensitive. Many letters used for CLI navigation and editing were chosen to provide an easy means of remembering their functions.

In *Table 1.2*, bolded characters inside the ***Function Summary*** column indicate the relationship between the letter used and the function.

Table 1.2 Key Combinations Used to Move the Cursor

Keystrokes	***Function Summary***	***Function Details***
Left Arrow or **Ctrl-B**	Back character	Moves the cursor one character to the left. When you enter a command extending beyond a single line, press the Left Arrow or Ctrl-B keys repeatedly to scroll back to the system prompt and verify the beginning of the command entry, or press the Ctrl-A key combination.
Right Arrow or **Ctrl-F**	Forward character	Moves the cursor one character to the right.
Esc, B	Back word	Moves the cursor back one word.
Esc, F	Forward word	Moves the cursor forward one word.
Ctrl-A	Beginning of line	Moves the cursor to the beginning of the line.
Ctrl-E	End of line	Moves the cursor to the end of the command line.
Ctrl-d		Deletes current character.
Ctrl-U		Deletes text up to cursor.
Ctrl-K		Deletes from cursor to end of line.
Ctrl-P		Gets the prior command from history.

Keystrokes	***Function Summary***	***Function Details***
Ctrl-N		Gets the next command from history.
Esc-C		Converts the rest of word to uppercase.
Esc-L		Converts the rest of word to lowercase.
Esc-D		Deletes the remainder of word.
Ctrl-W		Deletes a word up to the cursor.
Ctrl-Z		Enters the command and retursn to the root prompt.
Ctrl-L		Refreshes the input line.

1.5.2 Completing a Partial Command Name

Enter the first few letters of the command and then press the **Tab** key if you do not remember the complete command name, or to reduce the amount of typing. The command line parser completes the command if the string entered is unique to the command mode. Use **Ctrl-I** if your keyboard does not have a Tab key.

The CLI recognizes a command once you have entered enough characters to make the command unique. For example, if you enter conf in privileged EXEC mode, the CLI associates your entry with the configure command only because the configure command begins with `conf.`

In the following example, the CLI recognizes the unique string for privileged EXEC mode of conf when the Tab key is pressed:

```
RFS7000# conf<Tab>
RFS7000# configure
```

When you use the command completion feature, the CLI displays the full command name. The command is not executed until you use the **Return** or **Enter** key. This way the command can be modified if the full command was not what you intended by abbreviation. Enter a set of characters that could indicate more than one command to list commands that begin with that set of characters.

Alternatively, enter a question mark (?) to obtain a list of commands that begin with that set of characters. Do not leave a space between the last letter you enter and the question mark (?).

For example, entering `co?` lists commands available in the current command mode:

```
RFS7000# co?
copy? commit
RFS7000# co
```

NOTE The characters entered before the question mark are reprinted to the screen to complete the command entry.

1.5.3 Deleting Entries

Use any of the following keystrokes to delete command entries:

Keystrokes	*Purpose*
Backspace	Deletes the character to the left of the cursor.
Ctrl-D	Deletes the character at the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-W	Deletes the word up to the cursor.
Esc, D	Deletes from the cursor to the end of the word.

1.5.4 Re-displaying the Current Command Line

It is easy to recall the current command line entry if the system suddenly displays a message when entering a command. To redisplay the current command line (refresh the screen), use the following keystroke:

Keystrokes	*Purpose*
Ctrl-L	Redisplays the current command line.

1.5.5 Command Output pagination

When working with the CLI, output often extends beyond the visible screen length. In such a case, `Press Any Key to Continue (Q to Quit)` displays at the bottom of the screen. To resume , press the **Return** key to scroll down one line, or press the **Spacebar** to display the next full screen of output.

1.5.6 Transposing Mistyped Characters

If you have mistyped a command entry, it is possible to transpose the mistyped characters. To transpose characters, use the following keystroke:

Keystrokes	*Purpose*
Ctrl-T	Transposes the character to the left of the cursor with the character located at the cursor.

1.5.7 Controlling Capitalization

CLI commands are generally case-insensitive, and are typically in lowercase. To change the capitalization of the commands, use any of the following key sequences:

Keystrokes	*Purpose*
Esc, C	Capitalizes the letters at the right of cursor.
Esc, L	Changes the letters at the right of cursor to lowercase.

2

Common Commands

This chapter explains the common CLI commands used amongst the USER EXEC and PRIV EXEC modes.

The PRIV EXEC command set contains the commands available in USER EXEC mode, some commands can be entered in either mode. Commands entered in either USER EXEC mode or PRIV EXEC mode are referred to as EXEC mode commands. If the user or privilege is not specified, the referenced command can be entered in either mode.

2.1 Common Commands

Table 2.1 summarizes commands common amongst many switch contexts and instance.

Table 2.1 Common commands amongst most contexts

Command	**Description**	**Ref.**
clrscr	Clears the display screen.	page 2-3
debug	Debugging functions.	page 2-4
exit	Ends the current mode and moves down to the previous mode.	page 2-10
help	Describes the interactive help system.	page 2-11
no	Negates a command or set defaults.	page 2-12
service	Service commands.	page 2-13
show	Shows running system information.	page 2-25
terminal	Sets terminal line parameters.	page 2-24

2.1.1 clrscr

▶ *Common Commands*

Use this command to clear the screen displaying and refresh the prompt (**#**).

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000#clrscr
```

2.1.2 debug

▶ Common Commands

Use this command to debug certificate management, ip, mobility and MSTP functionalities.

Syntax (User Exec)

```
debug [certmgr (all|error|info)|ip (https|ssh)|
mobility (cc|error|forwarding <MAC Address>|mu|packet|peer|system)|
mstp (all|cli|packet|protocol|timer)]
```

Syntax (Priv Mode)

```
debug [all|cc|ccstats|certmgr|dhcpsvr|imi|ip|logging|mgmt|mobility|mstp|nsm|
pktdrvr|pm|radius|redundancy|securitymgr]
```

Parameters (User Exec)

certmgr (all|error|info)	Debugs certificate manager messages. • all – Traces error and informational messages from the Certificate Manager. • error – Traces error messages from the Certificate Manager. • info – Traces informational messages from the Certificate Manager.
ip (https|ssh)	Debugs Internet Protocol parameters. • https – Secure HTTP (HTTPS) server. • ssh – Secured Shell (SSH) server.
mobility (cc|error|forwarding <MAC Address>| mu|packet|peer|system)	Debugs L3 Mobility parameters. • cc – Debugs cc server events. • error – Debugs mobility errors. • forwarding <MAC Address> – Dataplane forwarding to MAC address of the mobile unit. • mu – MU events and state changes. • packet – Control packets. • peer – Peer establishment. • system – System events.
mstp (all|cli|packet|protocol| timer)	Debugs *Multiple Spanning Tree Protocol* (MSTP) parameters. • all – Debugs MSTP parameters. • cli – Debugs MSTP CLI commands. • packet – Debugs MSTP packets. • protocol – Debugs MST Protocol. • timer – Debugs MSTP timers.

Parameters (Priv Mode)

all	Enables debugging.
cc [access-port|all|al tap-detect| capwap| cluster|config|dot11|eap| ids|kerberos| l3-mob|media|mobile-unit|radio|radius| self-heal|snmp| system|wips|wisp] (debug|err|info|warn)	Cell controller (wireless) debugging messages. • access-port – Access port logs. • all – All modules. • alt – Address lookup logs. • ap-detect – Rogue AP detection logs. • capwap – Capwap logs. • cluster – Cluster related logs. • config – Configuration change logs. • dot11 – Datapath logs. • eap – 802.1x/eap logs. • ids – Intrusion detection logs. • kerberos – Kerberos logs. • l3-mob – Layer3 mobility logs. • media – Encapsulation media logs. • mobile-unit – Mobile unit logs. • radio – Radio logs. • radius – RADIUS client logs. • self-heal – Self Healing logs. • snmp – SNMP logs. • system – System call logs. • wips – WIPS sensor logs. • wisp – WISP logs. • debug – All messages (default). • err – Error and higher severity messages. • info – Information and higher severity messages. • warn – Warning and higher severity messages.
ccstats <module name>	Cellcontroller (wireless) debugging messages. • <module name> – CCStats Module to be debugged.
certmgr [all|error|info]	Certificate Manager debugging messages. • all – Traces error and informational messages from the Certificate Manager. • error – Traces error messages from the Certificate Manager. • info – Traces informational messages from the Certificate Manager.

dhcpsvr [all|error|info]	DHCP Conf Serv er Debugging Messages. • all – Traces error and info messages from the DHCP Conf Server. • error – Traces error messages from the DHCP Conf Server. • info – Traces informational messages from the DHCP Conf Server.
imi [all|cli-client|cli-server|errors|init|ntp]	Integrated Management Interface. • all – All debugging. • cli-client – CLI responses from protocol modules to IMI server. • cli-server – CLI commands from IMI server to protocol module. • errors – Errors. • init – Initialization process. • ntp – NTP debug messages.
ip [https|ssh]	Internet Protocol (IP). • https – *Secure HTTP* (HTTPS) server. • ssh – *Secured Shell* (SSH) server.
logging [all|errors|init|monitor|subagent]	Modify message logging facilities. • all – All debugging. • errors – Errors. • init – Logging module initialization. • monitor – Logging to monitors. • subagent – Sub-agent.
mgmt [all|debug|err|info|sys|warning]	Mgmt daemon. • all • debug • err • info • sys • warning

mobility [all|cc|error|forwarding <MAC Address>| mu|packet|peersystem]	L3 Mobility. • all – All debugging (except "forwarding"). • cc – ccserver events. • error – Error. • forwarding – Dataplane forwarding. • <MAC Address> – MAC address of the mobbile unit. • mu – MU events and state changes. • packet – Control Packets. • peer – Peer establishment. • system – System events.
mstp [all|cli|packet|protocol| timer]	*Multiple Spanning Tree Protocol* (MSTP). • all • cli • packet • protocol • timer
nsm [all|events|kernel|packet]	*Network Service Module* (NSM). • all • events • kernel • packet
pktdrvr [rate-limit|skip-packet-filter]	Pktdrvr (kernel wireless) debugging messages. • rate-limit – Log message rate-limiting. • skip-packet-filter – Do not call the packet filtering API when receiving or transmitting frames.
pm [all|errors|heartbeats|init |proc|shutdown| subagent|sys]	Process Monitor. • all • errors • heartbeats • init • proc • shutdown • subagent • sys

radius [all|err|info|warn]	RADIUS server debugging messages. • all – Traces all messages from the RADIUS server. • err – Traces error messages from the local RADIUS server. • info – Traces error, warning and informational messages from the RADIUS server. • warn – Traces error and warning messages from the RADIUS server.
redundancy [all|ccmsg|config|errors|general|heartbeats|init|packets|proc|shutdown|states|subagent|timer|warnings]	Redundancy protocol debugging messages. • all – Debugging all. • ccmsg – Msg exchange with CC. • config – Configuration processing. • errors – Errors. • general – General. • heartbeats – Heartbeats processing. • init – Redundancy initialization. • packets – Packet processing. • proc – Process flow. • shutdown – Shutdown process. • states – Redundancy state machine. • subagent – Sub-agent. • timer – Timer handling. • warnings – Warnings.
securitymgr [all|debug|error|ikeerror|ipsec|pmdebug|pmerror]	Security manager debugging messages. • all – Traces all messages from the Security Manager. • debug – Traces general debug messages from the Security Manager. • error – Traces general error messages from the Security Manager. • ikeerror – Traces debug messages for IKE. • ipsec – Traces Policy Manager messages. • pmdebug – Traces debug messages for the Policy Manager. • pmerror – Traces error messages for the Policy Manager.

Example

```
RFS7000#debug cc all
RFS7000#configure t
Enter configuration commands, one per line.  End with CNTL/Z.
RFS7000(config)#logging console 7
RFS7000(config)#Mar 15 15:41:47 2008: CC: cluster: portal unadopted. portal count
now: 7
Mar 15 15:41:47 2008: CC: cluster: tx-to-wccp ap: 4, radio: 7, mu: 0, rogue: 0,
sheal: 0, max-ap: 256
Mar 15 15:41:47 2008: CC: cluster: portal unadopted. portal count now: 6
Mar 15 15:41:47 2008: CC: cluster: tx-to-wccp ap: 4, radio: 6, mu: 0, rogue: 0,
sheal: 0, max-ap: 256
Mar 15 15:41:47 2008: CC: rfp: RF Port <00-A0-F8-CD-ED-C4> removed
Mar 15 15:41:47 2008: CC: alt: removing rfport <00-A0-F8-CD-ED-C4>
Mar 15 15:41:47 2008: CC: cluster: ap unadopted. ap count now: 3
Mar 15 15:41:47 2008: CC: cluster: tx-to-wccp ap: 3, radio: 6, mu: 0, rogue: 0,
sheal: 0, max-ap: 256
Mar 15 15:41:47 2008: CC: cluster: standy mode. Igoring Hello/Discovery at
attempts 1
Mar 15 15:41:47 2008: CC: CW_Rx_Discovery()-2815: Ignoring discovery attempts 1
from <00-A0-F8-CD-ED-C4>
Mar 15 15:41:47 2008: CC: CW_Add_Unadopted_AP()-2735: <00-A0-F8-CD-ED-C4> Added
to unadopted AP list
Mar 15 15:41:47 2008: CC: cluster: updating license count to 507
Mar 15 15:41:47 2008: %KERN-6-INFO: Prtl <00-A0-F8-CD-F5-64> rem @ 6.
Mar 15 15:41:48 2008: CC: cluster: standy mode. Igoring Hello/Discovery at
attempts 1
Mar 15 15:41:48 2008: CC: CW_Rx_Discovery()-2815: Ignoring discovery attempts 1
from <00-A0-F8-CD-ED-C4>
Mar 15 15:41:49 2008: CC: cluster: standy mode. Igoring Hello/Discovery at
attempts 1
Mar 15 15:41:49 2008: CC: CW_Rx_Discovery()-2815: Ignoring discovery attempts 1
from <00-A0-F8-CD-ED-C4>
Mar 15 15:41:49 2008: CC: cluster: portal unadopted. portal count now: 5
Mar 15 15:41:49 2008: CC: cluster: tx-to-wccp ap: 3, radio: 5, mu: 0, rogue: 0,
sheal: 0, max-ap: 256
Mar 15 15:41:49 2008: CC: cluster: portal unadopted. portal count now: 4
Mar 15 15:41:49 2008: CC: cluster: tx-to-wccp ap: 3, radio: 4, mu: 0, rogue: 0,
sheal: 0, max-ap: 256
Mar 15 15:41:49 2008: CC: rfp: RF Port <00-A0-F8-CD-ED-A4> removed
Mar 15 15:41:49 2008: CC: alt: removing rfport <00-A0-F8-CD-ED-A4>
Mar 15 15:41:49 2008: CC: cluster: ap unadopted. ap count now: 2
Mar 15 15:41:49 2008: CC: cluster: tx-to-wccp ap: 2, radio: 4, mu: 0, rogue: 0,
sheal: 0, max-ap: 256
Mar 15 15:41:49 2008: CC: cluster: standy mode. Igoring Hello/Discovery at
attempts 1
Mar 15 15:41:49 2008: CC: CW_Rx_Discovery()-2815: Ignoring discovery attempts 1
from <00-A0-F8-CD-ED-A4>
Mar 15 15:41:49 2008: CC: CW_Add_Unadopted_AP()-2735: <00-A0-F8-CD-ED-A4> Added
to unadopted AP list
Mar 15 15:41:49 2008: CC: cluster: updating license count to 508
Mar 15 15:41:50 2008: CC: cluster: standy mode. Igoring Hello/Discovery at
attempts 1
Mar 15 15:41:50 2008: CC: CW_Rx_Discovery()-2815: Ignoring discovery attempts 1
from <00-A0-F8-CD-ED-A4>
Mar 15 15:41:51 2008: CC: cluster: standy mode. Igoring Hello/Discovery at
attempts 1
Mar 15 15:41:51 2008: CC: CW_Rx_Discovery()-2815: Ignoring discovery attempts 1
from <00-A0-F8-CD-ED-A4>

RFS7000(config)#
```

2.1.3 exit

▶ Common Commands

Use this command to end the current mode and move to the previous mode.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config)#exit
```

2.1.4 help

▶ *Common Commands*

Use this command to get access to the advanced help feature. Use "**?**" anytime at the command prompt to get access to the help topic.

Two styles of help are provided:

1. Full help is available when ready to enter a command argument and describe each possible argument. There is a space between the command and ?, (e.g. 'show ?') .
2. Partial help is provided when an abbreviated argument is entered and you want to know what arguments match the input. There is no space between the command and ?, (For example, 'show ve?').

Syntax

```
help
```

or

```
?
```

Parameters

None.

Example

```
RFS7000>show ?
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  commands              Show command lists
  debugging             Debugging information outputs
  environment           show environmental information
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   MAC access-list assignment
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the switch.
  redundancy-members    Display redundancy group members in detail
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         spanning-tree Display spanning tree information
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000>show

RFS7000>show autoinstall ?
  |  Output modifiers
  >  Output redirection
  >>  Output redirection appending
```

2.1.5 no

Common Commands

Use this command to either negate a command or set its defaults.

Syntax

```
no
```

Parameters

None.

Example

```
RFS7000(config)#no ?
  access-list    Internet Protocol (IP)
  autoinstall    autoinstall configuration command
  banner         Reset login banner to nothing
  bridge         Bridge group commands
  country-code   Clear the currently configured country code. All existing
                 radio configuration will be erased
  crypto         Encryption related commands
  debug          Debugging functions
  ftp            Configure FTP Server
  hostname       Reset system's network name to default
  interface      Delete a virtual interface
  ip             Internet Protocol (IP)
  line           Configure a terminal line
  logging        Modify message logging facilities
  management     sets properties of the management interface
  ntp            Configure NTP
  prompt         Reset system's prompt
  radius-server  RADIUS server configuration commands
  redundancy     Configure redundancy group parameters
  service        Service Commands
  snmp-server    Modify SNMP engine parameters
  timezone       Revert the timezone to default (UTC)
  username       Establish User Name Authentication
  wlan-acl       Remove an ACL from a WLAN port

RFS7000(config)#no bridge  multiple-spanning-tree
RFS7000(config)#

RFS7000(config)#no bridge  instance <1-15> priority
RFS7000(config)#

RFS7000(config)#no bridge  forward-time
RFS7000(config)#

RFS7000(config)#no bridge  hello-time
RFS7000(config)#

RFS7000(config)#no bridge  max-age
RFS7000(config)#

RFS7000(config)#no bridge  max-age
RFS7000(config)#

RFS7000(config)#no bridge  spanning-tree portfast bpdu-filter
RFS7000(config)#

RFS7000(config)#no bridge  spanning-tree portfast bpduuard
RFS7000(config)#

RFS7000(config)#no bridge  spanning-tree errdisable-timeout enable
RFS7000(config)#

RFS7000(config)#no bridge  spanning-tree errdisable-timeout interval
RFS7000(config)#
```

2.1.6 service

▶ *Common Commands*

Use this command to service/debug the RFS7000 Switch.

Syntax (User Exec)

```
service [diag|encrypt|locator|save-cli|show]

service diag [enable|identify|limit|period <100-30000>|watchdog]
service diag limit [buffer(128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k)<0-
65535> |
fan <1-3>|filesys (etc2|flash|var)|
inodes (etc2|flash|var)|load (1|15|5)|maxFDs <0-32767>|
pkbuffers <0-65535>|procRAM < 0.0-100.0>|ram <0.0-25.0>|
routecache <0-65535>|temperature <1-8>]

service encrypt (secret)<2> LINE

service show [cli|command-history|crash-info|diag|info|memory|process|
reboot-history|startup-log|upgrade-history]
```

Parameters (User Exec Only)

diag	Diagnostics.
enable	Enable in service diagnostics.
identify	Identify this switch by flashing the LEDs.
limit {*buffer* (*128*|*128k*|*16k*|*1k*|*256*|*2k*|*32*|*32k*|*4k*|*512*|*64*|*64k*|*8k*) *<0-65535>*	Use this parameter to set the diagnostic limit submodes/commands. Configure the buffer usage warning limit. The warning limit can be set to one of the following sizes: • buffer – Buffer usage warning limit. • 128 – 128 byte buffer limit. • 128k – 128k byte buffer limit. • 16k – 16k byte buffer limit. • 1k – 1k byte buffer limit. • 256 – 256 byte buffer limit. • 2k – 2k byte buffer limit. • 32 – 32 byte buffer limit. • 32k – 32k byte buffer limit. • 4k – 4k byte buffer limit. • 512 – 512 byte buffer limit. • 64 – 64 byte buffer limit. • 64k – 64k byte buffer limit. • 8k – 8 byte buffer limit. • <0-65535> – Buffer usage warning limit 0-65535.
fan <1-3>	Use this parameter to set the fan speed limit. Configure the fan speed limit for both fans or just one of them.

filesys (etc2|flash|var)	Use this parameter to set the file system freespace limit. Select the freespace limit for the following sub context: • etc2 • flash • ram
inodes (etc2|flash|var)	File system inode limit. Select the freespace limit for the following sub context: • etc2 • flash • ram
load (1|15|5)	Configures the aggregate processor load. Select from the following submodes: • 1 – Aggregate processor load during the previous minute. • 15 – Aggregate processor load during the previous 15 minute. • 5 – Aggregate processor load during the previous 5 minute.
maxFDs <0-32767>	Configures the maximum number of file descriptors. Set anything between 0 to 32767 file descriptors.
pkbuffers <0-65535>	Configures and set the packet buffer head cache limit. Set anything between 0 to 65535 as the buffer cache limit.
procRAM < 0.0-100.0>	Defines the RAM space used by a process. Set the percentage of RAM space to be used by the processor from anything between 0.0 to 100.0 percent.
ram <0.0-25.0>	Configures the free space for the RAM. Configure the free space to anything between 0.0 to 100.0 percent.
routecache <0-65535>	Defines the IP route cache usage. Set with a value between 0 - 65553.
temperature <1-8>	Sets the switch temperature sensor. Set as many as 8 temperature sensors.
period <100-30000>	Sets the diagnostic period. • <100-30000> – Configures the diagnostics period. Set a value between 100-30000 milli seconds. The default value is 1000 milliseconds.
watchdog	Enables the watchdog.
encrypt(secret) 2 LINE	Encrypts passwords with a secret phrase using SHA256-AES256 encryption.
save-cli	Create's a file (clitree.html), which saves and displays the CLI tree for all modes.

show {*cli*|*command-history*|*crash-info*|*diag*|*info*|*memory*|*process*|*reboot-history*|*startup-log*|*upgrade-history*}	Displays the running system information. • *cli* – Shows CLI tree of current mode. • *command-history* – Displays a command (except show commands) history. • *crash-info* – Displays information about core, panic and access port dump files. • *diag* – Diagnostics. • *info* – Shows snapshot of available support information. • *memory* – Shows memory statistics. • *natstats* – Shows ACL rule stats. • *process* – Shows processes (sorted by memory usage). • *reboot-history* – Shows reboot history. • *rulestats* – Shows ACL rule stats. • *startup-log* – Shows the startup log. • *upgrade-history* – Shows the upgrade history.

Syntax (Priv Exec)

```
service [clear|copy|diag|diag-shell|encrypt|locator|save-
cli|securitymgr|show|start-shell|wireless]

service clear [all|aplogs|clitree|cores|dumps|panics|
pm(statistics|sys-restart-count)|
securitymgr (flows)[<0-349>|WORD|all|fe|ge|sa|tunnel|vlan]]

service copy (tech-support)[FILE|URL]

service diag [enable|identify|limit|period|watchdog]
service diag limit [buffer (128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k)
<0-65535>|fan <1-3> (low)|filesys (etc2|flash|var)|
inodes (etc2|flash|var)|load (1|15|5)|maxFDs <0-32767>|
pkbuffers <0-65535>|procRAM <0.0-100.0>|ram <0.0-25.0>|
routecache <0-65535>|temperature <1-8> (critical|high|low)]

service encrypt (secret)<2> LINE

service securitymgr [dump-core|enable-http-stats]

service show [cli|command-history|crash-info|diag|info|last-
passwd|memory|pm|process|reboot-history|securitymgr|startup-log|upgrade-
history|wireless]

service wireless [clear-ap-log <1-256>|dump-core |dump-state|
map-radios <1-127>|rate-scale|request-ap-log <1-256>|save-ap-log]
```

Parameters (Priv Exec mode only)

clear [all|aplogs|clitree|cores| dumps|panics| pm (statistics|sys-restart-count)| securitymgr (flows) [<0-349>|WORD| all|fe|ge|sa|tunnel|vlan]]	Resets different functions. • all – Removes all core, dump and panic files. • aplogs – Removes all ap log files. • clitree – Removes clitree.html (created by the save-cli command). • cores – Removes all core files. • dumps – Removes all dump files. • panics – Removes all kernel panic files. • pm (statistics|sys-restart-count) – Process Monitor. • securitymgr (flows) [<0-349>|WORD| all|fe|ge|sa|tunnel|vlan]] – Securitymgr parameters.
copy (tech-support) [FILE|URL]	Copies from one file to another. • tech-support – Copies extensive system information useful to technical support for troubleshooting. • FILE – Target file to copy. • URL – Target URL to copy.
diag [enable|identify|limit| period|watchdog]	Use this parameter as a diagnostics tool. • enable – Enables service diagnostics. • identify – Identifies this switch by flashing the LEDs. • limit – Diagnostic limit command. • buffer (128|128k|16k|1k|256|2k|32|32k|4k|512|64|64k|8k) <0-65535> – Buffer usage warning limit. • fan <1-3> – Fan speed limit of the fan number. • filesys (etc2|flash|var) – File system freespace limit. • inodes (etc2|flash|var) – File system inode limit. • load (1|15|5) – Agregate processor load during the previous minutes, based on the option selected. • maxFDs <0-32767> – Maximum number of file descriptors. • pkbuffers <0-65535> – Packet buffer head cache. • procRAM <0.0-100.0> – Percent RAM used by a process. • ram <0.0-25.0> – Percent free RAM. • routecache <0-65535> – IP route cache usage. • temperature <1-8> (critical|high|low) – Temperature limit. • period <100-30000> – Set diagnostics period. The default period is set as 1000 milliseconds. • watchdog – Enable the watchdog.

encrypt (secret) <2> LINE	Encrypt passwords with secret phrase, using a SHA256-AES256 type of encryption.
securitymgr [dump-core|enable-http-stats]	Securitymgr parameters. • dump-core – Create a core file of the securitymgr process. • enable-http-stats – Enable securitymgr HTTP statistics interface.
show [cli|command-history|crash-info|diag|info|last-passwd|memory|pm|process|reboot-history|securitymgr|startup-log|upgrade-history|wireless]	Displays running system information. • cli – Displays CLI tree of current mode. • command-history – Displays command (except show commands) history. • crash-info – Displays information about core, panic and AP dump files. • diag – Diagnostics. • info – Displays snapshot of available support information. • last-passwd – Displays the last password used to enter shell. • memory – Shows memory statistics. • pm – Displays process monitor details. • process – Displays processes (sorted by memory usage). • reboot-history – Displays reboot history. • securitymgr – Displays security manager details. • startup-log – Displays startup log. • upgrade-history – Displays upgrade history. • wireless – Displays wireless parameters details.
wireless [clear-ap-log <1-256>|dump-core |dump-state|map-radios <1-127>|rate-scale|request-ap-log <1-256>|save-ap-log]	Wireless parameters. • clear-ap-log – Clears ap logs. • dump-core – Creates a core file of the ccsrvr process. • dump-state – Creates a `ccsrvr.dump` file in nvram with internal state information. • map-radios – Sets radio-to-cpu mapping constant. • rate-scale – Enables wireless rate scaling (default). • request-ap-log – Requests access port log. • save-ap-log – Saves a debug/error log sent by the access port.

Syntax (Global Config)

```
service [advanced-vty|dhcp|password-encryption (secret)2 LINE|pm (max-sys-
restarts <1-5> |sys-restart)|prompt(crash-info)|
radius (restart)|set (command-history <10-300>|reboot-history <10-100>|
upgrade-history <10-100>)|show (cli)|terminal-length <0-512>]
```

Parameters(Global Config)

advanced-vty	Enables advanced mode vty interface.
dhcp	Enables the DHCP server service.
password-encryption (secret)2 LINE	Encrypts passwords. • secret (2) – Encrypts passwords with secret phrase, using SHA256-AES256 encryption. • LINE – Enter a passphrase for encryption.
pm (max-sys-restarts <1-5> | sys-restart)	Process Monitor. • max-sys-restarts <1-5> – Maximum number a process monitor must restart the system due to a failed processes. • sys-restart – Enables the process monitor to restart the system when a process fails.
prompt (crash-info)	Enables crash-info prompt.
radius (restart)	Enables the RADIUS Server.
set (command-history <10-300>|reboot-history <10-100>| upgrade-history <10-100>)	Set service parameters. • command-history <10-300> – Sets the size of the command history. The default value is 200. • reboot-history <10-100> – Sets the size of the reboot history. The default value is 50. • upgrade-history <10-100> – Sets the size of the upgrade history. The default value is 50.
show (cli)	Displays running system information. • cli – Shows the CLI tree of current mode.
terminal-length <0-512>	System wide terminal length configuration. • <0-512> – Number of lines of VTY (0 means no line control).

Example

```
RFS7000#service diag ?
  enable  Enable in service diagnostics
  led     LED control
  limit   diagnostic limit command
  period  Set diagnostics period

RFS7000#service diag enable

RFS7000#service diag limit ?
  buffer       buffer usage warning limit
  fan          Fan speed limit
  filesys      file system freespace limit
  load         agregate processor load
  maxFDs       maximum number of file descriptors
  pkbuffers    packet buffer head cache
  procRAM      percent RAM used by a process
  ram          percent free RAM
  routecache   IP route cache usage
  temperature  temperature limit
```

```
RFS7000#service diag limit buffer ?
  128   128 byte buffer limit
  128k  128k byte buffer limit
  16k   16k byte buffer limit
  1k    1k byte buffer limit
  256   256 byte buffer limit
  2k    2k byte buffer limit
  32    32 byte buffer limit
  32k   32k byte buffer limit
  4k    4k byte buffer limit
  512   512 byte buffer limit
  64    64 byte buffer limit
  64k   64k byte buffer limit
  8k    8k byte buffer limit

RFS7000#service diag limit buffer 32k ?
  <0-65535>  buffer usage warning limit 0-65535

RFS7000#service diag limit buffer 32k 4096

RFS7000#service diag limit fan ?
  <1-3>  Fan number

RFS7000#service diag limit fan 1 ?
  low  Low speed limit

RFS7000#service diag limit fan 1 low ?
  <1000-15000>  Limit value from 1000 to 15,000

RFS7000#service diag limit fan 1 low 1100
RFS7000#service diag limit fan 2 low 10000
RFS7000#Sep 01 15:51:54 2006: %DIAG-4-FANUNDERSPEED: Fan case under speed: 8881
RPM is under limit 10000 RPM

RFS7000#service diag limit filesys ?
  etc2   /etc2 file system
  flash  /flash file system
  ram    /ram file system

RFS7000#service diag limit filesys flash ?
  WORD  limit from 0.0 to 100.0

RFS7000#service diag limit filesys flash 20
RFS7000#service diag limit filesys etc2 10
RFS7000#service diag limit filesys ram 30

RFS7000#service diag limit load ?
  1   during the previous minute
  15  during the previous 15 minutes
  5   during the previous five minutes

RFS7000#service diag limit load 5 ?
  WORD  percentage load from 0.0 to 100.0

RFS7000#service diag limit load 5 50

RFS7000#service diag limit maxFDs ?
  <0-32767>  0-32767

RFS7000#service diag limit maxFDs 30000

RFS7000#service diag limit pkbuffers ?
  <0-65535>  limit from 0-65535

RFS7000#service diag limit pkbuffers 4096

RFS7000#service diag limit procRAM ?
  WORD  limit from 0.0-100.0
RFS7000#service diag limit procRAM 10

RFS7000#service diag limit ram ?
  WORD  limit from 0.0-100.0
```

```
RFS7000#service diag limit ram 20

RFS7000#service diag limit routecache ?
  <0-65535>  limit from 0-65535

RFS7000#service diag limit routecache 10240

RFS7000#service diag limit temperature ?
  <1-8>  temperature sensor number

RFS7000#service diag period ?
  <100-30000>  Diagnostics period <100-30000> default 1000 milliseconds

RFS7000#service diag period 20000

RFS7000#service save-cli

/usr/scripts/genclitree.sh: /usr/scripts/genclitree.sh: 15: eth: not found
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
RFS7000#

RFS7000>service show cli
User Exec mode:
+-autoinstall
  +-cluster-config
    +-enable [autoinstall (config|cluster-config|image) enable]
    +-url
      +-LINE [autoinstall (config|cluster-config|image) url LINE]
  +-config
    +-enable [autoinstall (config|cluster-config|image) enable]
    +-url
      +-LINE [autoinstall (config|cluster-config|image) url LINE]
  +-image
    +-enable [autoinstall (config|cluster-config|image) enable]
    +-url
      +-LINE [autoinstall (config|cluster-config|image) url LINE]
  +-start [autoinstall start]
+-clear
............

RFS7000>service show command-history
Configured size of command history is 200

  Date & Time          User  Location   Command
=====================================================================
Aug 31 23:40:15 2006   (null)     vty 131     wireless
Aug 31 23:40:15 2006   (null)     vty 131     config t
Aug 31 23:40:15 2006   (null)     vty 131     enable
Aug 31 23:40:14 2006   (null)     vty 131     interface eth0
Aug 31 23:40:14 2006   (null)     vty 131     config t
Aug 31 23:40:14 2006   (null)     vty 131     enable
Aug 31 23:40:13 2006   (null)     vty 131     line console 0
Aug 31 23:40:13 2006   (null)     vty 131     config t
Aug 31 23:40:13 2006   (null)     vty 131     enable
Aug 31 23:40:12 2006   (null)     vty 131     config t
Aug 31 23:40:12 2006   (null)     vty 131     enable
Aug 31 23:40:11 2006   (null)     vty 131     enable
Aug 31 16:30:14 2006   (null)     con 0     configure terminal
Aug 31 16:30:04 2006   (null)     con 0     en
Aug 31 16:29:21 2006   (null)     con 0     exit
Aug 30 19:54:13 2006   (null)     vty 130     enable
Aug 30 19:53:09 2006   (null)     vty 130     disable
Aug 30 19:41:12 2006   (null)     vty 130     clear mobility peer-statistics
157.235.208.39
```

```
RFS7000>service show crash-info

Coredump files:
Name                    Size    Date & Time
=============================================
imish_8990_200B.core.gz 299.5k   Aug 31 23:50

RFS7000>

RFS7000>service show info

4.0M out of 4.0M available for logs.
9.7M out of 11.4M available for history.
16.1M out of 18.6M available for crashinfo.

List of Files:

imish_8990_200B.core.gz         299.5k  Aug 31 23:50
messages.log                    200     Aug 30 15:32
snmpd.log                       316     Aug 30 15:33
startup.log                     16.5k   Aug 30 15:32
command.history                 9.6k    Aug 31 23:40
reboot.history                  2.3k    Aug 30 15:32
upgrade.history                 782     Aug 29 18:32

Please export these files or delete them for more space.

RFS7000>

RFS7000>service show memory
MemTotal:       256220 kB
MemFree:        155628 kB
Buffers:          1596 kB
Cached:          27912 kB
SwapCached:          0 kB
Active:          53832 kB
Inactive:        16272 kB
HighTotal:           0 kB
HighFree:            0 kB
LowTotal:       256220 kB
LowFree:        155628 kB
SwapTotal:           0 kB
SwapFree:            0 kB
Dirty:               0 kB
Writeback:           0 kB
Mapped:          50768 kB
Slab:             9984 kB
CommitLimit:    128108 kB
Committed_AS:    75368 kB
PageTables:        468 kB
VmallocTotal:   778200 kB
VmallocUsed:     19568 kB
VmallocChunk:   757824 kB
RFS7000>

RFS7000>service show process
  PID  STATUS   RSS  PPID %CPU %MEM COMMAND
  320  S        10M     1  0.0  4.1 ccsrvr
  345  S       8488     1  1.9  3.3 ccstatsd
  387  S       5612     1  0.0  2.1 securitymgr
  318  S       4480     1  0.0  1.7 snmpd
  394  S       3932     1  0.0  1.5 imi
  349  R       3424     1  0.0  1.3 isDiag
  367  S       3264   279  0.0  1.2 radconfd
  315  S       3208   279  0.0  1.2 CertMgr
  391  S       3104     1  0.0  1.2 radiusd
  373  S       2844     1  0.0  1.1 dhcpsvr
  319  S       2744     1  0.0  1.0 licenseMgr
 6823  S       2712   429  0.0  1.0 imish
 6770  S       2668     1  0.0  1.0 imish
  363  S       1824     1  0.0  0.7 nsm
  339  S       1736   279  0.0  0.6 fileMgmt
  291  S       1676     1  0.0  0.6 logd
  375  S       1672     1  0.0  0.6 wccpd
  279  S       1636     1  0.0  0.6 pmd
  430  S       1636     1  0.0  0.6 stunnel
 1370  S       1512     1  0.0  0.5 sshd
  346  S       1448     1  0.0  0.5 mobd
  340  S       1308   279  0.0  0.5 fileXferd.................


RFS7000> service show reboot-history
Configured size of reboot history is 50

  Date & Time             Event
=====================================================
Aug 30 15:32:39 2006     startup
Aug 30 15:31:17 2006     shutdown (graceful:user)
Aug 30 13:31:13 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 29 18:40:38 2006     startup
Aug 29 18:39:15 2006     shutdown (graceful:user)
Aug 28 12:38:09 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 23 13:33:02 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 21 13:10:09 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 17 15:10:21 2006     startup
Aug 17 15:08:58 2006     shutdown (graceful:user)
Aug 16 13:48:41 2006     startup
- - -                   shutdown (ungraceful:unexpected cold restart)
Aug 11 19:32:55 2006     startup
Aug 11 19:31:32 2006     shutdown (graceful:user)

RFS7000> service show startup-log
Aug 30 15:32:43 2006: %KERN-5-NOTICE: Linux version 2.6.13.4-ws-symbol (wios-
eng@wios-build) (gcc version 3.4.5) #1.
Aug 30 15:32:43 2006: %KERN-6-INFO: BIOS-provided physical RAM map:.
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 0000000000000000 -
000000000009fc00 (usable).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 000000000009fc00 -
00000000000a0000 (reserved).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000000e0000 -
0000000000100000 (reserved).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 0000000000100000 -
000000000ff40000 (usable).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 000000000ff40000 -
000000000ff50000 (ACPI data).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 000000000ff50000 -
0000000010000000 (ACPI NVS).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000fec80000 -
00000000fec81000 (reserved).
Aug 30 15:32:43 2006: %KERN-6-INFO:  BIOS-e820: 00000000fff80000 -
0000000100000000 (reserved).
Aug 30 15:32:43 2006: %KERN-5-NOTICE: 255MB LOWMEM available..
Aug 30 15:32:43 2006: KERN: On node 0 totalpages: 65344.
Aug 30 15:32:43 2006: KERN:   DMA zone: 4096 pages, LIFO batch:1.
Aug 30 15:32:43 2006: KERN:   Normal zone: 61248 pages, LIFO batch:31.
Aug 30 15:32:43 2006: KERN:   HighMem zone: 0 pages, LIFO batch:1.
Aug 30 15:32:43 2006: %KERN-6-INFO: DMI 2.3 present..
Aug 30 15:32:43 2006: KERN: ACPI: RSDP (v000 ACPIAM
) @ 0x000f7720.
Aug 30 15:32:43 2006: KERN: ACPI: RSDT (v001 A M I  OEMRSDT  0x09000512 MSFT
0x00000097) @ 0x0ff40000.
Aug 30 15:32:43 2006: KERN: ACPI: FADT (v002 A M I  OEMFACP  0x09000512 MSFT
0x00000097) @ 0x0ff40200.
Aug 30 15:32:43 2006: KERN: ACPI: MADT (v001 A M I  OEMAPIC  0x09000512 MSFT
0x00000097) @ 0x0ff40300.
Aug 30 15:32:43 2006: KERN: ACPI: OEMB (v001 A M I  OEMBIOS  0x09000512 MSFT
0x00000097) @ 0x0ff50040.
Aug 30 15:32:43 2006: KERN: ACPI: DSDT (v001  1ABVF 1ABVF007 0x00000007 INTL
0x02002026) @ 0x00000000.
```

```
RFS7000> service show upgrade-history
Configured size of upgrade history is 50

  Date & Time            Old Version     New Version     Status
=====================================================================
Aug 29 18:30:43 2006 3.0.0.0-180B 3.0.0.0-200B Successful
Aug 17 15:07:03 2006 3.0.0.0-17872X 3.0.0.0-180B Successful
Aug 11 19:29:41 2006 3.0.0.0-170B 3.0.0.0-17872X Successful
Aug 11 19:28:52 2006 3.0.0.0-170B 3.0.0.0-170B Unable to get update file. tftp:
server says: File not found
Aug 09 17:30:25 2006 3.0.0.0-17174X 3.0.0.0-170B Successful
Jul 26 15:17:14 2006 3.0.0.0-140D 3.0.0.0-17174X Successful
Jul 26 15:16:40 2006 3.0.0.0-140D 3.0.0.0-140D Unable to get update file. tftp:
server says: File not found
Jul 26 15:16:08 2006 3.0.0.0-140D 3.0.0.0-140D Unable to get update file. tftp:
C: Unknown host
Jul 19 19:52:38 2006 3.0.0.0-16786X 3.0.0.0-140D Successful
Jul 19 19:52:07 2006 3.0.0.0-16786X 3.0.0.0-16786X Unable to get update file.
tftp: server says: File not found
RFS7000>
```

2.1.7 terminal

▶ *Common Commands*

Use this command to set the length /number of lines displayed on the terminal window.

Syntax

```
terminal[length <0-512>|no(length <0-512>|width)|width <0-512> ]
```

Parameters

length	Sets the number of lines on a screen.
no	Negates a command or sets its defaults.
width	Sets the width/number of characters on a screen line.

Example

```
RFS7000>terminal length 100
RFS7000>

RFS7000>terminal width 200
RFS7000>
```

2.2 show

▶ *Common Commands*

This command displays the settings for the specified system component. There are a number of ways to invoke the show command:

- Invoked without any arguments, show displays information about the current context. If the current context contains instances, then show command (usually) displays a list of these instances.
- Invoked with the display_parameter, it displays information about that component.

Syntax

```
show [display_parameter]
```

Parameters

Display Parameters	***Description***	***Mode***	***Example***
autoinstall	Displays the autoinstall configuration.	Common	page 2-28
banner	Displays “Message of the Day” login banner.	Common	page 2-29
commands	Displays a command lists.	Common	page 2-30
debugging	Debugs information outputs.	Common	page 2-32
environment	Displays environmental information.	Common	page 2-34
history	Displays the session command history.	Common	page 2-34
interfaces	Displays interface status and configuration.	Common	page 2-35
ip	Displays the Internet Protocol.	Common	page 2-37
ldap	Displays LDAP server configuration parameters.	Common	page 2-41
licenses	Displays installed licenses, if any.	Common	page 2-42
logging	Displays the log configuration and buffer.	Common	page 2-43
mac	Displays the media access control IP configuration.	Common	page 2-44
mac-address-table	Display the MAC address table	Common	page 2-45
management	Displays the L3 management interface name.	Common	page 2-46
mobility	Displays mobility parameters.	Common	page 2-47
ntp	Displays the network time protocol.	Common	page 2-49
privilege	Displays the current privilege level.	Common	page 2-50
radius	Displays RADIUS configuration commands.	Common	page 2-51
redundancy-group	Displays redundancy group parameters.	Common	page 2-52

Display Parameters	***Description***	***Mode***	***Example***
redundancy-history	Displays the switch state transition history.	Common	page 2-54
redundancy-members	Displays redundancy group members in detail.	Common	page 2-55
snmp	Displays SNMP engine parameters.	Common	page 2-56
snmp-server	Displays SNMP engine parameters.	Common	page 2-57
spanning-tree	Displays spanning-tree information.	Common	page 2-59
static-channel-group	Displays the contents of static channel group membership.	Common	page 2-61
terminal	Displays terminal configuration parameters.	Common	page 2-62
timezone	Displays the timezone.	Common	page 2-63
users	Displays information about terminal lines.	Common	page 2-64
version	Displays the software and hardware version.	Common	page 2-65
wireless	Displays wireless configuration commands.	Common	page 2-66
wlan-acl	Displays wlan based ACL information.	Common	page 2-96
access-list	Displays access list Internet Protocol (IP) configuration.	Privilege/Global Config	page 2-73
aclstats	Displays ACL statistics.	Privilege/Global Config	page 2-74
alarm-log	Displays the alarms currently in the system.	Privilege/Global Config	page 2-75
boot	Displays the boot configuration.	Privilege/Global Config	page 2-76
clock	Displays the system clock.	Privilege/Global Config	page 2-77
debugging	Displays debug settings.	Privilege/Global Config	page 2-78
dhcp	Displays DHCP Server configuration.	Privilege/Global Config	page 2-79
environment	Displays environmental information.	Privilege/Global Config	page 2-33
file	Displays filesystem information.	Privilege/Global Config	page 2-81

Display Parameters	***Description***	***Mode***	***Example***
ftp	Displays the FTP Server configuration.	Privilege/Global Config	page 2-82
password-encryption	Displays the password's encryption settings.	Privilege/Global Config	page 2-83
running-config	Displays the current operating configuration.	Privilege/Global Config	page 2-84
securitymgr	Displays debug info for ACL, VPN and NAT.	Privilege/Global Config	page 2-87
sessions	Displays active open (current) connections.	Privilege/Global Config	page 2-88
spanning-tree	Display spanning tree information.	Privilege/Global Config	page 2-89
startup-config	Displays the contents of the startup configuration.	Privilege/Global Config	page 2-93
static-channel-group	Displays the static channel group membership.	Privilege/Global Config	page 2-94
upgrade-status	Displays last image upgrade status.	Privilege/Global Config	page 2-95
wlan-acl	Displays WLAN based ACL.	Privilege/Global Config	page 2-96

2.2.1 autoinstall

▶ *Common to all modes*

Syntax

```
show autoinstall
```

Parameters

None.

Example

```
RFS7000>show autoinstall
RFS7000>
```

2.2.2 banner

▸ *Common to all modes*

Syntax

```
show banner
```

Parameters

motd	Enters the *Message of the Day* banner.

Example

```
RFS7000>show banner motd
Welcome to CLI
RFS7000>
```

2.2.3 commands

▶ *Common to all modes*

Syntax

```
RFS7000>show commands
```

Parameters

None.

Example

```
RFS7000>show commands
  clear mobility event-log (mobile-unit|peer)
  clear mobility event-log (mobile-unit|peer)
  clear mobility mobile-unit (AA-BB-CC-DD-EE-FF|home-database|foreign-
database|all)
  clear mobility mobile-unit (AA-BB-CC-DD-EE-FF|home-database|foreign-
database|all)
  clear mobility mobile-unit (AA-BB-CC-DD-EE-FF|home-database|foreign-
database|all)
  clear mobility mobile-unit (AA-BB-CC-DD-EE-FF|home-database|foreign-
database|all)
  clear mobility peer-statistics (A.B.C.D|)
  clear mobility peer-statistics (A.B.C.D|)
  clear spanning-tree detected-protocols
  clear spanning-tree detected-protocols interface INTERFACE
  clrscr
  cluster-cli enable
  debug certmgr ( error|info|all )
  debug certmgr ( error|info|all )
  debug certmgr ( error|info|all )
  debug ip https
  debug ip ssh
  debug mobility (cc|error|forwarding (AA-BB-CC-DD-EE-FF|)|mu|packet|peer|system)
  debug mobility (cc|error|forwarding (AA-BB-CC-DD-EE-FF|)|mu|packet|peer|system)
  debug mobility (cc|error|forwarding (AA-BB-CC-DD-EE-FF|)|mu|packet|peer|system)
  debug mobility (cc|error|forwarding (AA-BB-CC-DD-EE-FF|)|mu|packet|peer|system)
  debug mobility (cc|error|forwarding (AA-BB-CC-DD-EE-FF|)|mu|packet|peer|system)
  debug mobility (cc|error|forwarding (AA-BB-CC-DD-EE-FF|)|mu|packet|peer|system)
  debug mobility (cc|error|forwarding (AA-BB-CC-DD-EE-FF|)|mu|packet|peer|system)
  debug mobility (cc|error|forwarding (AA-BB-CC-DD-EE-FF|)|mu|packet|peer|system)
  debug mstp all
  debug mstp cli
  debug mstp packet rx
  debug mstp packet tx
  debug mstp protocol
  debug mstp protocol detail
  debug mstp timer
  debug mstp timer detail
  disable
  enable
  (exit|logout|quit)
  h
  help
  lo
(exit|logout|quit)
  no cluster-cli enable
  no debug certmgr ( error|info|all )
  no debug certmgr ( error|info|all )
  no debug certmgr ( error|info|all )
  no debug ip https
  no debug ip ssh
  no debug mstp all
  no debug mstp cli
  no debug mstp packet rx
  no debug mstp packet tx
  no debug mstp protocol
  no debug mstp protocol detail
  no debug mstp timer
  no debug mstp timer detail
  no page
  no service diag enable
  no service diag period
  no service diag watchdog
  no service locator
  p
  page
  (exit|logout|quit)
  show autoinstall
  show autoinstall status
  show banner motd
  show commands
  show debugging
  show debugging mstp
  show environment
  show history
.....................................................(contd)

RFS7000>
```

2.2.4 debugging

▶ *Common to all modes*

Syntax

```
show debugging (mstp)
```

Parameters

mstp	Displays information related to the *Multiple Spanning Tree Protocol* (MSTP).

Example

```
RFS7000(config)#show debugging mstp
MSTP debugging status:
RFS7000(config)#
```

2.2.5 environment

- *Common to all modes*

Syntax

```
show environment
```

Parameters

None.

Example

```
RFS7000>show environment
                   upwind of CPU temperature :  30.0 C
                         CPU die temperature :  53.0 C
                       left side temperature :  30.0 C
                         by FPGA temperature :  29.0 C
                     front right temperature :  27.0 C
                      front left temperature :  27.0 C
                           fan 1 fan         :  6540 rpm
                           fan 2 fan         :  6660 rpm
                           fan 3 fan         :  6420 rpm
RFS7000>
```

2.2.6 history

▶ *Common to all modes*

Syntax

```
show history
```

Parameters

None.

Example

```
RFS7000>show history
   1 show
   2 clrscr
   3 enable
   4 clrscr
   5 configure terminal
   6 exit
   7 clrscr
   8 show history
RFS7000>
```

2.2.7 interfaces

▶ *Common to all modes*

Syntax

```
show interfaces [<name>|fe|ge <1-4>|sa <1-4>|
switchport(<name>|fe|ge|sa|tunnel|vlan)|tunnel <1-32>|vlan <1-4094>]
```

Parameters

IFNAME	Interface name.
fe	FastEthernet interface.
ge <1-4>	GigabitEthernet interface. Select an index value between 1- 4.
sa <1- 4>	StaticAggregate interface. Select an index value between 1- 4.
switchport ()	Status of Layer2 interfaces. Select from the following L2 interfaces: • *fe* – FastEthernet interface. • *ge* – GigabitEthernet interface. • *sa* – StaticAggregate interface. • *tunnel* – Tunnel interface. • *vlan* – VLAN.
tunnel <1-32>	Tunnel interface. Select an index value between 1- 32.
vlan <1-4092>	VLAN interface. Select an index value between 1- 4092.

Example

```
RFS7000(config)#show interfaces fe
Interface fe
  Hardware Type Ethernet, Interface Mode Layer 3, address is 00-15-70-37-fc-93
  index=1, metric=1, mtu=1500, (PAL-IF)  <UP,BROADCAST,RUNNING,MULTICAST>
  Speed: Admin Auto, Operational 100M, Maximum 100M
  Duplex: Admin Auto, Operational Full
  Active Medium: Copper
  inet 157.235.208.122/24 broadcast 157.235.208.255
    input packets 229359, bytes 61627914, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 7096, bytes 703376, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
RFS7000(config)#
RFS7000(config)#show interfaces ge 1
Interface ge1
  Hardware Type Ethernet, Interface Mode Layer 2, address is 00-15-70-37-fc-8f
  index=2001, metric=1, mtu=1500, (HAL-IF)  <UP,BROADCAST,MULTICAST>
  Speed: Admin Auto, Operational Unknown, Maximum 1G
  Duplex: Admin Auto, Operational Unknown
  Active Medium: Unknown
  Switchport Settings: Mode: Access, Access Vlan: 1
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
RFS7000(config)#

RFS7000(config)#show interfaces sa 2
Interface sa2
  Hardware Type AGGREGATE, Interface Mode Layer 2, address is 00-15-70-37-fc-91
  index=2005, metric=1, mtu=0, (HAL-IF)  <>
  Speed: Admin Auto, Operational Unknown, Maximum 1G
  Duplex: Admin Auto, Operational Unknown
  Active Medium: Unknown
  Switchport Settings: Mode: Access, Access Vlan: 1
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
RFS7000(config)#

RFS7000(config)#show interfaces switchport fe
Interface fe
  Switchport Settings: Mode: Access, Access Vlan: 0
RFS7000(config)#

RFS7000(config)#show interfaces switchport ge 1
Interface ge1
  Switchport Settings: Mode: Access, Access Vlan: 1
RFS7000(config)#

RFS7000(config)#show interfaces vlan 1
Interface vlan1
  Hardware Type VLAN, Interface Mode Layer 3, address is 00-15-70-37-fc-8f
  index=5, metric=1, mtu=1500, (PAL-IF)  <UP,BROADCAST,RUNNING,MULTICAST>
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 2147, bytes 742862, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
RFS7000(config)#
```

2.2.8 ip

Common to all modes

Syntax

```
show ip [access-group (IFNAME | eth <1-2> | vlan <1-4094>) |access-list |arp |
ddns(binding)| dhcp (binding|pool)| dhcp-vendor-options | domain-name |
http(secure-server|server)| interface(IFNAME|brief|tunnel|vlan) |
name-server |
nat (interfaces|translations[inside|outside][destination|source])|
route(A.B.C.D|A.B.C.D/M|detail) | routing | ssh | telnet ]

show ip access-group (IFNAME|eth <1-2> |vlan <1-4094>)
Show ip access-group <interface-name>
show ip arp
show ip ddns(binding)
show ip dhcp(binding|pool)
show ip dhcp-vendor-options
show ip domain-name
show ip http(secure-server|server)
show ip interface(IFNAME|brief|tunnel|vlan)
show ip name-server
show ip nat [interfaces|translations(inside|outside)(destination|source)]
show ip route(A.B.C.D|A.B.C.D/M|detail)
show ip routing
show ip ssh
show ip telnet
```

Parameters

access-group	Displays the ACLs attached to an interface.
IFNAME	The interface name to which the ACL is associated. It lists the details of ACLs configured on the particular Layer 3 or Layer 2 interface.
eth	The name of the Ethernet interface to which the ACL is associated.
vlan	The name of the VLAN interface to which the ACL is associated.
access-list	Lists IP access lists.
arp	Displays Address Resolution Protocol.
ddns	Displays DDNS configuration.
binding	DNS Address bindings.
dhcp	Displays the DHCP Server configuration.
binding	DNS Address bindings.
pool	DHCP pools.
dhcp-vendor-options	DHCP Option 43 parameters received from DHCP server.
domain-name	Default domain for DNS.
http	Hyper Text Transfer Protocol.
secure-server	Secure HTTP server.
server	HTTP server.
interface	IP interface status and configuration.

IFNAME	Interface name.
brief	Brief summary of IP status and configuration.
tunnel	Tunnel interface.
vlan	VLAN interface.
name-server	DNS nameservers.
nat ( )	Network Address Translation (NAT). • interfaces – NAT Configuration on Interfaces. • translations – NAT translations. • inside|outside (destination|source).
route	IP routing table.
A.B.C.D	Displays the network in the IP routing table.
A.B.C.D/M	IP prefix <network>/<length>, e.g., 35.0.0.0/8.
detail	IP routing table in detail.
routing	IP routing status.
ssh	*Secured Shell* (SSH) server.
telnet	Telnet server.

Usage Guidelines

1. It has been noted the interface and VLAN status is displayed as UP despite of a disconnection. In such a case, shutdown the VLAN. Follow these steps:

   a. Check the status of the interface and VLAN:

   ```
   RFS7000(config)#show ip interface brief
   Interface             IP-Address            Status                Protocol
   vlan1                 157.235.208.69(DHCP)   up                    up
   vlan3                 unassigned             up                    up
   RFS7000(config)#
   ```

   b. If the stauts of the VLAN is UP (even if interfaces are diconnected), shutdown the VLAN associated with fe1:

   ```
   RFS7000(config)*#show ip interface brief
    Interface           IP-Address/Mask        Status             Protocol
     fe                   157.235.208.122/24(DHCP) up                   up
     vlan1                unassigned(DHCP)        up                   up
     vlan200              unassigned              up                   up
    RFS7000(config)*#shutdown
   ```

   c. Check the status and note if the VLAN has been disassociated. Its status has now changed to DOWN.

   ```
   RFS7000(config)#show ip interface brief
   Interface             IP-Address            Status                Protocol
   ```

```
vlan1                 157.235.208.69(DHCP)  up                    up
vlan3                 unassigned            administratively down down
RFS7000(config)#
```

2. The above instance may occur when a DHCP interface is disconnected. DHCP is not effected because it runs on a virtual interface and not on the physical interface. In this case, it is the physical interface that is disconnected not the virtual interface.
   When the Ethernet interface comes back up, it restarts the DHCP client on any of the virtual interfaces (SVIs) in which the physical interface is a member port. This ensures (if the interface was disconnected and reconnected to a different interface), it gets a new ip address, route, name server, domain name etc. corresponding to the new DHCP server/ scope.

Example

```
RFS7000(config)*#show ip access-group all
Interface fe
  Inbound IP Access List :
  Inbound MAC Access List :
Interface ge1
  Inbound IP Access List :
  Inbound MAC Access List :
Interface ge2
  Inbound IP Access List :
  Inbound MAC Access List :
Interface ge3
  Inbound IP Access List :
  Inbound MAC Access List :
Interface ge4
  Inbound IP Access List :
  Inbound MAC Access List :
Interface vlan1
  Inbound IP Access List :
Interface vlan200
  Inbound IP Access List :
RFS7000(config)*#

RFS7000(config)#show ip access-list
Standard IP access list 20
    mark 8021p 5 any rule-precedence 10
RFS7000(config)#

RFS7000#show ip dhcp binding
IP              MAC/Client-Id      Type       Expiry Time
--              -------------      ----       -----------

RFS7000(config)#show ip dhcp binding
IP              MAC/Client-Id      Type       Expiry Time
--              -------------      ----       -----------
RFS7000(config)#

RFS7000#show ip dhcp pool
!
ip dhcp pool pl
!
ip dhcp pool pool1
 domain-name test.com
 bootfile 123
 network 10.10.10.0/24
 address range 10.10.10.2 10.10.10.30
!
ip dhcp pool poo110
 next-server 1.1.1.1
 netbios-node-type b-node

RFS7000#show ip dhcp-vendor-options
Server Info:
Firmware Image File:
Config File:
Cluster Config File:
```

```
RFS7000#show ip domain-name
 IP domain-lookup : Enable
 Domain Name   : symbol.com

RFS7000#show ip http server
HTTP server: Running
Config status: Enabled

RFS7000#show ip http secure-server
HTTP secure server: Running
Config status: Enabled
Trustpoint: default-trustpoint

RFS7000#show ip interface brief
Interface             IP-Address            Status                Protocol
vlan1                 157.235.208.233(DHCP)  up                    up
tunnel1               unassigned             up                    up

RFS7000#show ip interface tunnel 1 ?
  brief  Brief summary of IP status and configuration

RFS7000#show ip interface tunnel 1 brief
Interface             IP-Address            Status                Protocol
tunnel1               unassigned             up                    up

RFS7000#show ip interface vlan 1 brief
Interface             IP-Address            Status                Protocol
vlan1                 157.235.208.233(DHCP)  up                    up

RFS7000#show ip name-server
157.235.3.195            dynamic
157.235.3.196            dynamic

RFS7000(config)#show ip nat interfaces
=======================
Interface   Direction
=======================
vlan1       UNKNOWN
vlan400     UNKNOWN
RFS7000(config)#

RFS7000(config)#show ip nat translations outside source
S/D Dir Actual Address              NATed Address          ACL       Overload-If
RFS7000(config)#

RFS7000#show ip routing
IP routing is on

RFS7000(config)#show ip route detail
Codes: K - kernel/icmp, C - connected, S - static, D - DHCP
       > - Active route,  - Next-hop in FIB, p - stale info

S       1.1.0.0/16 [1/0] via 1.1.1.1 inactive
S       1.1.1.0/24 [1/0] via 1.1.1.2 inactive
S       10.0.0.0/8 [1/0] via 10.10.10.10 inactive
S       157.235.208.0/24 [1/0] via 157.235.208.246 inactive

RFS7000#show ip ssh
SSH server: enabled
Status: running
Keypair name: default_ssh_rsa_key
Port: 22

RFS7000#show ip telnet
Telnet server: enabled
Status: running
Port: 23
```

2.2.9 ldap

▶ *Common to all modes*

Syntax

```
show ldap(configuration(primary|secondary))
```

Parameters

ldap	LDAP server.
configuration	LDAP server configuration parameters.
primary	Primary LDAP server.
secondary	Secondary LDAP server.

Example

```
RFS7000(config-radsrv)#show ldap configuration
LDAP Server Config Details
--------------------------

Primary LDAP Server configuration

        IP Address             : 10.10.10.1
        Port                   : 369
        Login                  :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
        Bind DN                : cn=kumar,ou=symbol,dc=activedirectory,dc=com
        Base DN                : ou=symbol,dc=activedirectory,dc=com
        Password               : 0 symbol@123
        Password Attribute     : UserPassword
        Group Name             : cn
        Group Membership Filter: (&(objectClass=group)(member=%{Ldap-UserDn}))
        Group Member Attr      : radiusGroupName
        Net timeout            : 1 second(s)

Secondary LDAP

        IP Address             : 10.10.10.5
        Port                   : 369
        Login                  :
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})
        Bind DN                : cn=kumar,ou=symbol,dc=activedirectory,dc=com
        Base DN                : ou=symbol,dc=activedirectory,dc=com
        Password               : 0 symbol@123
        Password Attribute     : UserPassword
        Group Name             : cn
        Group Membership Filter: (&(objectClass=group)(member=%{Ldap-UserDn}))
        Group Member Attr      : radiusGroupName
        Net timeout            : 1 second(s)
```

2.2.10 licenses

Common to all modes

Syntax

```
show licenses
```

Parameters

None.

Example

```
RFS7000(config)#show licenses
  feature usage    license string                license value     usage
    AP               2FFD7fE9 CD016155 14A92C70              48      1
```

2.2.11 logging

▶ *Common to all modes*

Syntax

```
show logging
```

Parameters

None.

Example

```
RFS7000(config)#show logging

Logging module: enabled
    Aggregation time: disabled
    Console logging: level debugging
    Monitor logging: disabled
    Buffered logging: level informational
    Syslog logging: disabled

Log Buffer (3840 bytes):

Feb 19 22:25:28 2007: %NSM-6-DHCPIP: Interface fe acquired IP address
157.235.208.122/24 via DHCP

Feb 19 21:33:09 2007: %KERN-6-INFO: fe: Setting full-duplex based on negotiated
link capability..

Feb 19 21:33:09 2007: %KERN-6-INFO: fe: DSPCFG accepted after 0 usec..

Feb 19 18:50:38 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: DNSALG:
Application gateway started.

Feb 19 18:50:38 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: FTPALG:
Application gateway started.

Feb 19 18:50:38 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: FTPALG: Shutting
down.

Feb 19 18:50:38 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: DNSALG: Shutting
down.

Feb 19 18:50:37 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: DNSALG:
Application gateway started.

Feb 19 18:50:37 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: FTPALG:
Application gateway started.

Feb 19 18:50:37 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: FTPALG: Shutting
down.

Feb 19 18:50:37 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: DNSALG: Shutting
down.

Feb 19 18:50:37 2007: %NSM-6-IFUP: Interface vlan400 is up

Feb 19 18:48:58 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: DNSALG:
Application gateway started.

Feb 19 18:48:58 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: FTPALG:
Application gateway started.

Feb 19 18:48:58 2007: %DAEMON-5-NOTICE: WIOS_SECURITYMGR[1109]: FTPALG: Shutting
down.
.................................................................................
......................................................................
RFS7000(config)#
```

2.2.12 mac

▶ *Common to all modes*

Syntax

```
show mac(access-list)
```

Parameters

access-list	Lists MAC access lists.

Example

```
RFS7000(config)#show mac access-list
RFS7000(config)#
```

2.2.13 mac-address-table

▶ *Common to all modes*

Syntax

```
show mac-address-table
```

Parameters

None.

Example

```
RFS7000#show mac-address-table
bridge       VLAN port      mac            fwd timeout
1            2    ifindex 0  0090.2762.c786 1    0
1            2    ifindex 0  0014.85a0.ebc4 1    0
1            2    ifindex 0  0008.7493.8134 1    0
1            2    ifindex 0  0008.c7eb.070b 1    0
1            2    ifindex 0  000d.56d1.742c 1    0
1            2    ifindex 0  000e.0c6e.ade7 1    0
1            5    ifindex 0  00a0.f8ea.4c99 1    0
1            2    ifindex 0  0080.a366.d7b6 1    0
1            2    ifindex 0  0011.2599.9b35 1    0
1            2    ifindex 0  0012.0197.3794 1    0
1            2    ifindex 0  0013.723c.ba60 1    0
1            1    vlan4     0015.7037.fac3 1    0
1            2    vlan4     0015.7037.fac3 1    0
1            3    vlan4     0015.7037.fac3 1    0
1            4    vlan4     0015.7037.fac3 1    0
1            5    vlan4     0015.7037.fac3 1    0
1            2    ifindex 0  000e.0c72.1922 1    0
1            2    ifindex 0  001a.6c82.fa91 1    0
1            2    ifindex 0  000f.8f19.ba18 1    0
1            2    ifindex 0  0080.a366.c36a 1    0
1            2    ifindex 0  000f.8f19.ba40 1    0
RFS7000#
```

2.2.14 management

▶ *Common to all modes*

Syntax

```
show management
```

Parameters

None.

Example

```
RFS7000(config)#show management
Mgmt Interface: vlan1
Management access permitted via any vlan interface
RFS7000(config)#
```

2.2.15 mobility

▸ *Common to all modes*

Syntax

```
show mobility [event-log|forwarding|global|mobile-unit|peer|statistics]

show mobility event-log [mobile-unit|peer]
show mobility forwarding (AA-BB-CC-DD-EE-FF)
show mobility mobile-unit [<AA-BB-CC-DD-EE-FF>|detail]
show mobility peer [<A.B.C.D>|detail]
show mobility statistics <AA-BB-CC-DD-EE-FF>
```

Parameters

event-log	Displays mobility event logs . • *mobile-unit* – MU event logs. • *peer* – Peer event logs.
forwarding	Mobile units in the forwarding plane. • *AA-BB-CC-DD-EE-FF* – MAC address of the mobile unit.
global	Global mobility parameters.
mobile-unit	Mobile units in the mobility database. • *AA-BB-CC-DD-EE-FF* – MAC address of the mobile unit. • *detail* – Displays detailed information.
peer	Mobility peers. • *A.B.C.D* – IP address of Peer. • *detail* – Displays detailed information.
statistics	Mobility statistics. • *AA-BB-CC-DD-EE-FF* – MAC address of the mobile unit.

Example

```
RFS7000(config)#show mobility ?
  event-log    Event Log
  forwarding   Mobile-unit information in the forwarding plane
  global       Global Mobility parameters
  mobile-unit  Mobile-units in the Mobility Database
  peer         Mobility peers
  statistics   Mobile-unit Statistics

RFS7000(config)#show mobility global
Mobility Global Parameters
Admin Status                     : DISABLED
Operational-Status               : DISABLED (Admin-status is DISABLED)
Local Address                    : 0.0.0.0
Port Number                      : 58788
Max Roam Period                  : 5 sec
Number of Peers                  : 0 (established=0)
Number of MUs                    : 0 (Home=0, Foreign=0, Fwding-plane=0, Delete-
pend=0)
L3-Mobility enabled WLANs        : NONE
RFS7000(config)#

RFS7000(config)#show mobility event-log mobile-unit
Time            Event        Evt-Src-IP      MU-Mac             MU-IP
HS-IP           CS-IP
```

```
09/14 19:17:52  IP-UPD-MU    n/a             00-0f-3d-e9-a6-54
157.235.208.134 157.235.208.16  157.235.208.16
09/14 19:17:51  ADD-MU       n/a             00-0f-3d-e9-a6-54  0.0.0.0
157.235.208.16  157.235.208.16
09/14 19:17:51  DEL-MU       n/a             00-0f-3d-e9-a6-54  0.0.0.0
157.235.208.16  157.235.208.16
09/14 19:17:50  ADD-MU       n/a             00-0f-3d-e9-a6-54  0.0.0.0
157.235.208.16  157.235.208.16

RFS7000>show mobility forwarding
Mac-Address        IP-Address       State       Tunnel             HS-Vlan
RFS7000>

RFS7000>show mobility global
Mobility Global Parameters
Admin-Status                      : DISABLED
Operational-Status                : DISABLED (Admin-status is DISABLED)
Local-Address                     : 0.0.0.0
Max-Roam-Period                   : 5 sec
Number of Peers                   : 0 (established=0)
Number of MUs                     : 0 (Home=0, Foreign=0, Delete-pend=0)
L3-Mobility enabled WLANs         : NONE
RFS7000>

RFS7000(config)#show mobility mobile-unit detail
HOME MU Database: Total=1
MU MAC-Address: 00-0f-3d-e9-a6-54, IP-Address: 157.235.208.134,
SSID=wios_rad_test1
  Home-Switch: 157.235.208.16, Current-Switch: 157.235.208.16, HS-VLAN=1

Foreign MU Database: Total=0

RFS7000(config)#show mobility peer detail
Mobility Peers: Total=1, Established=0
Peer: 1.1.1.1, State: PASSIVE-CONNECTING
  Join-Sent  : 0      Join-Rcvd  : 0      Leave-Sent : 0      Leave-Rcvd : 0
  Rehome-Sent: 0      Rehome-Rcvd: 0      L3roam-Sent: 0      L3roam-Rcvd: 0
  Num-flaps  : 0      Connect-retries: 0    Peer-Uptime: 0 days, 00:00:00

RFS7000(config)#show mobility statistics

MU <00-0f-3d-e9-a6-54> Mob-State HS_AND_CS
-----------------------------------------------
Inter-          |Rx                                         |Tx
face            |unicast    MC         BC         Error     |unicast    MC
BC         Error
wlan_port        0          0          0          0          0          0
0          0
```

2.2.16 ntp

▶ *Common to all modes*

Syntax

```
show ntp (association (detail)|status)
```

Parameters

ntp	Network time protocol.
association	NTP associations.
detail	Displays NTP association details.
status	Displays NTP status.

Example

```
RFS7000>show ntp associations
  address         ref clock       st  when  poll  reach  delay  offset    disp
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
RFS7000>(config)#

RFS7000(config)#show ntp status
Clock is synchronized, stratum 0, actual frequency is 0.0000 Hz, precision is 2^0
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 0.000 msec,
RFS7000(config)#

RFS7000(config)#show ntp associations detail
157.235.208.105 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
our mode client, peer mode unspec, our poll intvl 6, peer poll intvl 10
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-20,
org time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
rcv time 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
xmt time c8b42a7e.6eb04252 (Sep 14 19:22:38 UTC 2006)
filtdelay =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filtoffset =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filterror =  16000.00  16000.00  16000.00  16000.00  16000.00  16000.00
16000.00  16000.00

RFS7000(config)#show ntp status
Clock is unsynchronized, stratum 16, reference is INIT
actual frequency is 0.0000 Hz, precision is 2**-20
reference time is 00000000.00000000 (Feb 07 06:28:16 UTC 2036)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 1395.000 msec,
```

2.2.17 privilege

▶ *Common to all modes*

Syntax

```
show privilege
```

Parameters

None.

Example

```
RFS7000>show privilege
Current user privilege: superuser
RFS7000>
```

2.2.18 radius

▶ *Common to all modes*

Syntax

```
show radius [configuration|eap(configuration)|group|nas( A.B.C.D/M)|proxy| rad-
user|trust-point]
```

Parameters

radius	RADIUS configuration commands.
configuration	RADIUS server configuration parameters.
eap (*configuration)*	EAP parameters and configuration.
group	RADIUS group configuration.
nas (A.B.C.D/M)	Enter a client IP address and mask.
proxy	Proxy information.
rad-user	RADIUS user information.
trust-point	RADIUS trust-point configuration.

Example

```
RFS7000(config)#show radius proxy
Proxy Details
_____________
Proxy retry delay : 6  seconds
Proxy retry count : 4

Proxy Realm Details
___________________
Realm   : symbol.com
        IP Address    : 10.10.10.5
        Port          : 1812
        Shared secret : 0 secret123
```

2.2.19 redundancy-group

▶ *Common to all modes*

Syntax

```
show redundancy-group [config|runtime]
```

Parameters

config	Displays redundancy group information.
runtime	Displays runtime redundancy group information.

Example

```
RFS7000(config)#show redundancy-group config

Redundancy Group Configuration Detail
Redundancy Feature                 : Disabled
Redundancy group ID                : 1
Redundancy Mode                    : Primary
Redundancy Interface IP            : 0.0.0.0
Number of configured peer(s)       : 0
Heartbeat-period                   : 5 Seconds
Hold-period                        : 15 Seconds
Discovery-period                   : 30 Seconds
Handle STP                         : Disabled
Switch Installed License           : 0
Switch running image version       : 1.0.0.0-228D

RFS7000(config)#

RFS7000>show redundancy-group runtime

Redundancy Group Runtime Information
Redundancy Protocol Version          : 2.0
Redundancy Group License             : 0
Cluster AP Adoption Count            : Not Applicable
Switch AP Adoption Count             : Not Applicable
Redundancy State                     : Disabled
Radio Portals adopted by Group       : Not Applicable
Radio Portals adopted by this Switch : Not Applicable
Rogue APs detected in this Group     : Not Applicable
Rogue APs detected by this Switch    : Not Applicable
MUs associated in this Group         : Not Applicable
MUs associated in this Switch        : Not Applicable
Radios in selfhealing mode           : Not Applicable
Selfhealing APs in this Switch       : Not Applicable
Group maximum AP adoption capacity   : Not Applicable
Switch Adoption capacity             : Not Applicable
Established Peer(s) Count            : Not Applicable
Redundancy Group Connectivity status : Not Applicable

RFS7000>

RFS7000(config)#show redundancy-group

Redundancy Group Configuration Detail
Redundancy Feature                 : Disabled
Redundancy group ID                : 1
Redundancy Mode                    : Primary
Redundancy Interface IP            : 0.0.0.0
Number of configured peer(s)       : 0
Heartbeat-period                   : 5 Seconds
Hold-period                        : 15 Seconds
Discovery-period                   : 30 Seconds
Handle STP                         : Disabled
Switch Installed License           : 0
Switch running image version       : 1.0.0.0-228D
```

```
Redundancy Group Runtime Information
Redundancy Protocol Version          : 2.0
Redundancy Group License             : 0
Cluster AP Adoption Count            : Not Applicable
Switch AP Adoption Count             : Not Applicable
Redundancy State                     : Disabled
Radio Portals adopted by Group       : Not Applicable
Radio Portals adopted by this Switch : Not Applicable
Rogue APs detected in this Group     : Not Applicable
Rogue APs detected by this Switch    : Not Applicable
MUs associated in this Group         : Not Applicable
MUs associated in this Switch        : Not Applicable
Selfhealing RPs in this Group        : Not Applicable
Selfhealing APs in this Switch       : Not Applicable
Group maximum AP adoption capacity   : Not Applicable
Switch Adoption capacity             : Not Applicable
Established Peer(s) Count            : Not Applicable
Redundancy Group Connectivity status : Not Applicable

RFS7000(config)#
```

2.2.20 redundancy-history

Common to all modes

Syntax

```
show redundancy-history
```

Parameters

None.

Example

```
RFS7000>show redundancy-history
State Transition History

Time                        Event Triggered       State
---------------------------------------------------------

Sep 06 18:20:56 2006        Redundancy Disabled   Disabled

RFS7000>
```

2.2.21 redundancy-members

▶ *Common to all modes*

Syntax

```
show redundancy-members (A.B.C.D)
```

Parameters

A.B.C.D	IP address of the member switch.

Example

```
RFS7000(config)#show redundancy-members brief

Member ID (Self)              : 10.10.10.10
Member State                  : Not Applicable

Member ID                     : 10.10.10.1
Member State                  : Peer Configured
```

2.2.22 snmp

▶ *Common to all modes*

Syntax

```
show snmp [user(snmpmanager|snmpoperator|snmptrap)]
```

Parameters

user	Displays the SNMP user.
snmpmanager	Shows manager information.
snmpoperator	Shows operator information.
snmptrap	Shows trap information.

Example

```
RFS7000(config)#show snmp user snmpmanager
userName      access   engineId                    Authentication  Encryption
snmpmanager   rw       80000184806b8b456745a3cccc  MD5             DES
RFS7000(config)#

RFS7000(config)#show snmp user snmpoperator
userName      access   engineId                    Authentication  Encryption
snmpoperator  ro       80000184806b8b456745a3cccc  MD5             DES
RFS7000(config)#

RFS7000(config)#show snmp user snmptrap
userName      access   engineId                    Authentication  Encryption
snmptrap      rw       80000184806b8b456745a3cccc  MD5             DES
RFS7000(config)#
```

2.2.23 snmp-server

▶ *Common to all modes*

Syntax

```
show snmp-server[traps(wireless-statistics( mobile-unit | radio |
wireless-switch | wlan))]
```

Parameters

traps	Displays trap enabled flags.
wireless-statistics	Displays wireless-stats rate traps.
mobile-unit	Displays mobile unit rate traps.
radio	Displays radio rate traps.
wireless-switch	Displays switch rate traps.
wlan	Displays WLAN rate traps.

Example

```
RFS7000>show snmp-server traps
----------------------------------------------------------------------
Global enable flag for Traps                                    N
----------------------------------------------------------------------
Enable flag status for Individual Traps
----------------------------------------------------------------------
Module Type               Trap Type                 Enabled?[Y/N]
----------------------------------------------------------------------
snmp                     coldstart                              N
snmp                     linkdown                               N
snmp                     linkup                                 N
snmp                     authenticationFail                     N
nsm                      dhcpIPChanged                          N
redundancy               memberUp                               N
redundancy               memberDown                             N
redundancy               memberMisConfigured                    N
redundancy               adoptionExceeded                       N
redundancy               grpAuthLevelChanged                    N
misc                     lowFsSpace                             N
misc                     processMaxRestartsReached              N
wireless station         associated                             N
wireless station         disassociated                          N
wireless station         deniedAssociationOnCapability          N
wireless station         deniedAssociationOnShortPream          N
wireless station         deniedAssociationOnSpectrum            N
wireless station         deniedAssociationOnErr                 N
wireless station         deniedAssociationOnSSID                N
wireless station         deniedAssociationOnRates               N
wireless station         deniedAssociationOnInvalidWPAWPA2IE    N
wireless station         deniedAssociationAsPortCapacityReached N
wireless station         tkipCounterMeasures                    N
wireless station         deniedAuthentication                   N
wireless station         radiusAuthFailed                       N
wireless radio           adopted                                N
wireless radio           unadopted                              N
wireless radio           detectedRadar                          N
wireless ap-detection    externalAPDetected                     N
wireless self-healing    activated                              N
wireless ids             excessiveAuthAssociation               N
wireless ids             excessiveProbes                        N
misc                     savedConfigModified                    N
RFS7000>

RFS7000>show snmp-server traps wireless-statistics mobile-unit
     pktsps-greater-than                          disabled
     tput-greater-than                        disabled
     avg-bit-speed-less-than                  disabled
     avg-signal-less-than                     disabled
     nu-percent-greater-than                  disabled
     gave-up-percent-greater-than             disabled
     avg-retry-greater-than                   disabled
     undecrypt-percent-greater-than           disabled
RFS7000>

RFS7000>show snmp-server traps wireless-statistics radio
     pktsps-greater-than                      disabled
     tput-greater-than                        disabled
     avg-bit-speed-less-than                  disabled
     avg-signal-less-than                     disabled
     nu-percent-greater-than                  disabled
     gave-up-percent-greater-than             disabled
     avg-retry-greater-than                   disabled
     undecrypt-percent-greater-than           disabled
     num-stations-greater-than                disabled
RFS7000>

RFS7000>show snmp-server traps wireless-statistics wireless-switch
     pktsps-greater-than                      disabled
     tput-greater-than                        disabled
     num-stations-greater-than                disabled
RFS7000>


RFS7000>show snmp-server traps wireless-statistics wlan
     pktsps-greater-than                      disabled
     tput-greater-than                        disabled
     avg-bit-speed-less-than                  disabled
     avg-signal-less-than                     disabled
     nu-percent-greater-than                  disabled
     gave-up-percent-greater-than             disabled
     avg-retry-greater-than                   disabled
     undecrypt-percent-greater-than           disabled
     num-stations-greater-than                disabled
RFS7000>
```

2.2.24 spanning-tree

▶ *Common to all modes*

Syntax

```
show spanning-tree mst
[config|detail (interface){<IF Name>|fe|ge <1-4>|sa <1-4>|tunnel <1-32> |vlan <1-
4094>}|instance <1-15>(interface){<IF Name>|fe|ge <1-4>|sa <1-4>|tunnel <1-32>
|vlan <1-4094>}]
```

Parameters

config	Displays MSTP configuration information.
detail (interface) {<IF Name>|fe|ge <1-4>| sa <1-4>|tunnel <1-32> | vlan <1-4094>}	Displays detailed interface information. • IF Name – Interface name. • fe – FastEthernet interface. • ge <1-4> – GigabitEthernet interface. • sa <1-4> – StaticAggregate interface. • tunnel <1-32> – Tunnel interface. • vlan <1-4094> – VLAN interface.
instance (interface <1-15>) {<IF Name>|fe|ge <1-4>| sa <1-4>|tunnel <1-32> | vlan <1-4094>}	Displays instance information. • IF Name – Interface name. • fe – FastEthernet interface. • ge <1-4> – GigabitEthernet interface. • sa <1-4> – StaticAggregate interface. • tunnel <1-32> – Tunnel interface. • vlan <1-4094> – VLAN interface.

Example

```
RFS7000>show spanning-tree mst config
%
%  MSTP Configuration Information for bridge 1 :
%-------------------------------------------------------
%  Format Id      : 0
%  Name           : My Name
%  Revision Level : 0
%  Digest         : 0xAC36177F50283CD4B83821D8AB26DE62
%-------------------------------------------------------
RFS7000>

RFS7000>show spanning-tree mst detail interface ge 1
% Bridge up - Spanning Tree Enabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 800000157037fbef
% 1: CIST Reg Root Id 800000157037fbef
% 1: CST Bridge Id 800000157037fbef
% portfast bpdu-filter enabled
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off
%   ge1: Port 2001 - Id 87d1 - Role Designated - State Forwarding
%   ge1: Designated External Path Cost 0 -Internal Path Cost 0
%   ge1: Configured Path Cost 200000  - Add type Explicit ref count 1
%   ge1: Designated Port Id 87d1 - CST Priority 128  -
%   ge1: CIST Root 800000157037fbef
%   ge1: Regional Root 800000157037fbef
%   ge1: Designated Bridge 800000157037fbef
%   ge1: Message Age 0 - Max Age 20
%   ge1: CIST Hello Time 2 - Forward Delay 15
%   ge1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge1: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   ge1: Portfast configured - Current portfast on
%   ge1: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge1: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   ge1: no root guard configured     - Current root guard off
%   ge1: Configured Link Type point-to-point - Current point-to-point
%
RFS7000>
```

2.2.25 static-channel-group

▶ *Common to all modes*

Syntax

```
show static-channel-group
```

Parameters

None.

Example

```
RFS7000>show static-channel-group
RFS7000>
```

2.2.26 terminal

▶ *Common to all modes*

Syntax

```
show terminal
```

Parameters

None.

Example

```
RFS7000(config)#show terminal
Terminal Type: vt102
Length: 42     Width: 125
RFS7000(config)#
```

2.2.27 timezone

▶ *Common to all modes*

Syntax

```
show timezone
```

Parameters

None.

Example

```
RFS7000>show timezone
Timezone is Etc/UTC
RFS7000>
```

2.2.28 users

▶ *Common to all modes*

Syntax

```
show users
```

Parameters

None.

Example

```
RFS7000(config)#show users
   Line     PID   User        Uptime       Location
   0 con 0  1003   admin       11:38m       ttyS0
 130 vty 0  27693   admin       10:21m       0
RFS7000(config)#
```

2.2.29 version

▶ *Common to all modes*

Syntax

```
show version (verbose)
```

Parameters

verbose	Displays software and hardware details.

Example

```
RFS7000(config)#show version
RFS7000 version 1.0.0.0-228D MIB=01a
Copyright (c) 2006 Symbol Technologies, Inc.
Booted from primary.

Switch uptime is 0 days, 5 hours 50 minutes
CPU is RMI Phoenix V0.4
255188 kB of on-board RAM
RFS7000(config)#

RFS7000(config)#show version verbose
RFS7000 version 1.0.0.0-228D MIB=01a
Copyright (c) 2006 Symbol Technologies, Inc.
Booted from primary.

Switch uptime is 0 days, 11 hours 53 minutes
CPU is RMI Phoenix V0.4
PCI bus 0 device 3 function 2
    USB Controller
    unknown mfg
    unknown
PCI bus 0 device 3 function 1
    USB Controller
    unknown mfg
    unknown
PCI bus 0 device 3 function 0
    USB Controller
    unknown mfg
    unknown
PCI bus 0 device 1 function 0
    Ethernet controller
    unknown mfg
    unknown
255188 kB of on-board RAM
RFS7000(config)#
```

2.2.30 wireless

Common to all modes

Syntax

```
show wireless [ap
(<1-48>|AA-BB-CC-DD-EE-FF)|
 ap-detection-config |
 ap-images |
 ap-unadopted |
 approved-aps |
 channel-power(11a {indoor|outdoor}|11b {indoor|outdoor}|
                 11bg {indoor|outdoor})|
 config |
 hotspot-config <1-32>|
 ids (filter-list)|
 mac-auth-local<1-1000> |
 mobile-unit (<1-4096>|AA-BB-CC-DD-EE-FF|
               association-history <MAC address>|
                probe-history [<1-200>|config-list]|
                radio <1-4096>| statistics|wlan)
 phrase-to-key (wep128 | wep64)|
 qos-mapping (wired-to-wireless | wireless-to-wired)|
 radio (<1-1000>|beacon-table|config(<1-1000>|default-11a|default-11b|
         default-11bg)|
 monitor-table |
 statistics (<1-1000|beacon-table|config|monitor-table|statistics)|
 regulatory (country codes)|
 self-heal-config <1-1000>|
 sensor (default-config | discovered-sensors)|
 unapproved-aps |
 wireless-switch-statistics (detail)|
 wlan (config {<1-32>|all|enabled}|
 statistics <1-32>)]
```

```
show wireless ap (<1-48>|AA-BB-CC-DD-EE-FF)
show wireless ap-detection-config
Show wireless ap-images
show wireless ap-unadopted
show wireless approved-aps
show wireless channel-power (11a (indoor | outdoor)| 11b (indoor |
                             outdoor)| 11bg indoor | outdoor))
show wireless config
show wireless hotspot-config <1-32 >
show wireless ids (filter-list)
show wireless mac-auth-local<1-1000>


show wireless mobile-unit (<1-4096> | AA-BB-CC-DD-EE-FF |
                           association-history <MAC address>|
                           probe-history [<1-200>|config-list]|
                              radio <1-4096>| statistics|wlan)

show wireless phrase-to-key (wep128 | wep64)
show wireless qos-mapping (wired-to-wireless | wireless-to-wired)
show wireless radio ( <1-1000> | beacon-table | config ( <1-1000> |
                      default-11a |default-11b | default-11bg)|
                       monitor-table | statistics)
show wireless regulatory (country codes)
show wireless self-heal-config <1-1000>
show wireless sensor (default-config | discovered-sensors)
show wireless unapproved-aps
show wireless wireless-switch-statistics (detail)
show wireless wlan (config( <1-32> | all | enabled)| statistics <1-32>)
```

Parameters

ap	Status of adopted access port.
<1-48>	The index of the access port.
AA-BB-CC-DD-EE-FF	The MAC address of a access port.
ap-detection-config	Detected AP configuration parameters.
ap-images	Lists the access port images on the switch.
ap-unadopted	Lists unadopted access ports.
approved-aps	Approved APs seen by access port scans.
channel-power	List of available channel and power levels for a radio.
11a	Radio is 802.11a.
11b	Radio is 802.11b.
11bg	Radio is 802.11bg.
indoor	Radio is placed indoors.
outdoor	Radio is placed outdoors.
config	Wireless configuration parameters.
hotspot-config	WLAN hotspot configuration.
<1-32>	A WLAN index <1-32>.
ids	Intrusion detection parameters.
filter-list	Displays the list of currently filtered mobile units.
mac-auth-local	List out the mac-auth-local entries.
<1-1000>	Displays mac-auth-local entry.
mobile-unit	Details of associated mobile unit.
<1-8192>	Index of mobile unit.
AA-BB-CC-DD-EE-FF	MAC address of mobile unit.
association-history <mac adress>	Displays mobile unit history. Enter the mobile unit MAC address in AA-BB-CC-DD-EE-FF format.
probe-history ( )	Displays MU probe-history. • <1-200> – Index to display probe-logging. • config-list – List probe history MAC addresses.
radio <1-4096>	Show mobile units associated with this radio. • <1-4096> – A single radio index.

statistics	Mobile unit rf statistics.
wlan <wlan_range>	Show mobile units associated to this WLAN. • <wlan_range> – A WLAN index between 1 to 256.
phrase-to-key	Displays the WEP keys generated by a passphrase.
wep128	Displays WEP128 keys.
wep64	Displays WEP64 keys.
qos-mapping	Quality of Service mappings used for mapping WMM access categories and 802.1p / DSCP tags.
wired-to-wireless	Mappings used when traffic is switched from wired to the wireless side.
wireless-to-wired	Mappings used when traffic is switched from wireless to the wired side.
radio	Radio related commands.
<1-1000>	A single radio index.
beacon-table	The radio-to-radio beacon table.
config	Radio configuration.
<1-1000>	A single radio index.
default-11a	Default 11a configuration template.
default-11b	Default 11b configuration template.
default-11bg	Default 11bg configuration template.
monitor-table	The radio-to-radio monitoring table.
statistics	Radio statistics.
regulatory	Regulatory (allowed channel/power) information for a particular country.
self-heal-config	Self healing Configuration Parameters.
<1-1000>	A single radio index.
all	All configured radios.
sensor	Wireless Intrusion Protection System parameters.
default-config	Default configuration parameters for sensors.
discovered-sensors	Sensor access ports discovered by the switch.
unapproved-aps	Unapproved APs seen by access port or mobile unit scans.
wireless-switch-statistics	Switch statistics.
detail	Detailed switch statistics.

wlan	Wireless LAN related parameters.
config	WLAN configuration.
<1-256>	A WLAN index <1-256>.
all	All WLANs in configuration.
enabled	Only WLANs currently enabled.
statistics	WLAN statistics.
<1-256>	A WLAN index <1-256>.

Example

```
RFS7000>show wireless ap
Number of access-ports adopted   : 0
Available licenses               : 0
Clustering enabled               : N
Clustering mode                  : primary
RFS7000>

RFS7000*>show wireless ap-detection-config
timeout                  : 300 seconds
mu-assisted scan         : disabled
mu-assisted scan refresh : 1800 seconds
configured approved-aps  :
Index | Bss Mac           | Ssid
-------------------------------------------------------
RFS7000*>

RFS7000>show wireless ap-images
  Idx   ap-type      Image-Name         Size (bytes)  Version
   1    ap300     WISP-AP300              293516      00.02-29
   2    ap300     WIAP-300                244076      01.00-1635b
   3    ap300     AP300-IDS-Sensor        295064      00.00-04
   4    ap100     AP100                   31034       02.05-00
   5    ap4131    AP4131                  191440      07.00-01
   6    ap4131    Revert-AP4131           665704      00.00-00
RFS7000>

RFS7000>show wireless ap-unadopted
RFS7000>

RFS7000>show wireless approved-aps
access-port detection is disabled
RFS7000>

RFS7000>show wireless channel-power 11a indoor
% Error: No valid channels or power levels
RFS7000>

RFS7000>show wireless config
country-code            : None
adoption-pref-id        : 1
proxy-arp               : enabled
adopt-unconf-radio      : enabled
dot11-shared-key-auth   : disabled
ap-detection            : disabled
oversized-frames        : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp fix windows        : disabled
broadcast-tx-speed      : optimize-for-throughput
smart-scan 11a channels :
smart-scan 11bg channels:
RFS7000>
```

```
RFS7000>show wireless hotspot-config

WLAN: 1 status: disabled description: WLAN1 ssid: 101
 Page-Location: simple
 Internal Pages
  Page-type : login
   Title : Login Page
   Header : Network Login
   Description : Please enter your username and password
   Footer : Contact the network administrator if you do not have an account
  Image URL main:
  Image URL small:

  Page-type : welcome
   Title : Authentication success.
   Header : Authentication Success.
   Description : You now have network access.<BR>Click the disconnect link below
to end this session.
   Footer :
  Image URL main:
  Image URL small:

  Page-type : fail
   Title : Unable to authenticate
   Header : Authentication Failed.
   Description : Either the username and password are invalid, or service is
unavailable at this time
   Footer : Contact the network administrator if you do not have an account
  Image URL main:
  Image URL small:

 External Pages
  Page-Type : login
   URL :
  Page-Type : welcome
   URL :
  Page-Type : fail
   URL :
Allow-list IP addresses

WLAN: 2 status: disabled description: WLAN2 ssid: 102
 Page-Location: simple
 Internal Pages
  Page-type : login
   Title : Login Page
 -- MORE --, next page: Space, next line: Enter, quit: Control-C
......................................................

RFS7000>show wireless ids
 detect-window               : 10 seconds

 Excessive Operations::  Threshold(mu radio switch)   Filter-Ageout
  probe-requests       :       0      0      0             60 Sec
  association-requests :       0      0      0             60 Sec
  disassociations      :       0      0      0             60 Sec
  authentication-fails :       0      0      0             60 Sec
  crypto-replay-fails  :       0      0      0             60 Sec
  80211-replay-fails   :       0      0      0             60 Sec
  decryption-fails     :       0      0      0             60 Sec
  unassoc-frames       :       0      0      0             60 Sec
  eap-starts           :       0      0      0             60 Sec


 Anomaly Detection::             Status     Filter-Ageout
  probe-requests           :   disabled      60 Sec
  association-requests     :   disabled      60 Sec
  disassociations          :   disabled      60 Sec
  authentication-fails     :   disabled      60 Sec
  crypto-replay-fails      :   disabled      60 Sec
  80211-replay-fails       :   disabled      60 Sec
  decryption-fails         :   disabled      60 Sec
  unassoc-frames           :   disabled      60 Sec
  eap-starts               :   disabled      60 Sec
  null-destination         :   disabled      60 Sec
  same-source-destination  :   disabled      60 Sec
  multicast-source         :   disabled      60 Sec
  weak-wep-iv              :   disabled      60 Sec
  tkip-countermeasures     :   disabled      60 Sec
  invalid-frame-length     :   disabled      60 Sec
RFS7000>

RFS7000>show wireless mac-auth-local 50
RFS7000>

RFS7000>show wireless mobile-unit statistics
% Error: None of the mobile-units are associated!!
```

2.2.31 wlan-acl

▶ *Common to all modes*

Syntax

```
show wlan-acl [<1-256>|all]
```

Parameters

<1-256>	Displays ACLs attached to the specified WLAN ID.
all	Displays ACLs attached to the WLAN port.

Example

```
RFS7000>show wlan-acl 200
WLAN port: 200
  Inbound IP Access List   :
  Inbound MAC Access List  :
  Outbound IP Access List  :
  Outbound MAC Access List :
RFS7000>

RFS7000>show wlan-acl all
RFS7000>
```

2.2.32 access-list

▶ *Priviledge / Global Config*

This command lists all the access lists (numbered and named) configured on the switch. The numbered access list displays all numbered ACLs. The named access-list displays the details of the name ACL.

Syntax

```
show access-list
show access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)
Show access-list <acl-name>
```

Parameters

<1-99>	IP standard access list.
<100-199>	IP extended access list.
<1300-1999>	IP standard access list (expanded range).
<2000-2699>	IP extended access list (expanded range).
WORD	Name of ACL.

Example

```
RFS7000(config)#show access-list
Extended IP access list 110
    permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
    permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
    permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
RFS7000(config)#


RFS7000(config)#show access-list 110
Extended IP access list 110
    permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
    permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
    permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
RFS7000(config)#
```

2.2.33 aclstats

Priviledge / Global Config

This command displays the statisitcs of all the access lists configured on the switch.

Syntax

```
aclstats [<name>|fe|ge <1-4>|sa <1-4>|tunnel <1-32>|vlan <1-4094>]
```

Parameters

IFNAME	Interface name.
fe	FastEthernet interface.
ge <1-4>	GigabitEthernet interface. Select an index value between 1-4.
sa <1- 4>	StaticAggregate interface.Select an index value between 1-4.
tunnel <1-32>	Tunnel interface. Select from an index value between 1-32.
vlan <1-4092>	VLAN interface. Select from an index value between 1- 4092.

Example

```
RFS7000(config)#interface fe
RFS7000(config-if)#

RFS7000(config)#interface ge 3
RFS7000(config-if)#

RFS7000(config)#interface sa 2
RFS7000(config-if)#

RFS7000(config)#interface tunnel 27
RFS7000(config-if)#

RFS7000(config)#interface vlan 400
RFS7000(config-if)#
```

2.2.34 alarm-log

▶ *Priviledge / Global Config*

Syntax

```
show alarm-log ( <1-65535>| acknowledged | all | count | new |
severity-to-limit( critical |informational | major | normal | warning))
```

Parameters

<1-65535>	Displays details for specific alarm Id.
acknowledged	Displays acknowledged alarms currently in the system.
all	Displays all alarms currently in the system.
count	Displays count of alarms currently in the system.
new	Displays new alarms currently in the system.
severity-to-limit	Displays alarms having a specified or higher severity.
critical	Displays critical alarms.
informational	Displays all informational or higher severity alarms.
major	Displays major or higher severity alarms.
normal	Displays normal or higher severity alarms.
warning	Displays warning or higher severity alarms.

Example

2.2.35 boot

▶ *Priviledge / Global Config*

Syntax

```
show boot
```

Parameters

None.

Example

```
RFS7000#show boot

Image           Build Date              Install Date          Version
-----       --------------------    --------------------      --------------
Primary     Feb 05 20:27:25 2007     Feb 13 19:29:28 2007     1.0.0.0-228D
Secondary   Jan 19 06:41:09 2007     Jan 23 20:14:19 2007     1.0.0.0-200D

Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
RFS7000#
```

2.2.36 clock

▶ *Priviledge / Global Config*

Syntax

```
show clock
```

Parameters

None.

Example

```
RFS7000#show clock
Sep 13 16:46:27 UTC 2006
RFS7000#
```

2.2.37 debugging

- *Priviledge / Global Config*

Syntax

```
show debugging (mstp)
```

Parameters

mstp	Displays MSTP debugging information.

Example

```
RFS7000#show debugging mstp
MSTP debugging status:
  MSTP all debugging is on
RFS7000#show debugging mstp
MSTP debugging status:
  MSTP all debugging is on
RFS7000#
```

2.2.38 dhcp

▶ *Priviledge / Global Config*

Use this command to display DHCP Server configurations.

Syntax

```
show dhcp [config|status]
```

Parameters

config	Displays DHCP server configuration.
status	Displays whether the DHCP server is running or not.

Example

```
RFS7000#show dhcp config

service dhcp
!
ip dhcp pool vlan63
 default-router 192.168.157.2
 network 192.168.63.0/24
 address range 192.168.63.20 192.168.63.30

RFS7000#
```

2.2.39 environment

Privilege / Global Config

Syntax

```
show environment
```

Parameters

None.

Example

```
RFS7000#show environment
                   upwind of CPU temperature :  33.0 C
                         CPU die temperature :  62.0 C
                       left side temperature :  31.0 C
                         by FPGA temperature :  30.0 C
                     front right temperature :  28.0 C
                      front left temperature :  29.0 C
                           fan 1 fan         :  6540 rpm
                           fan 2 fan         :  6600 rpm
                           fan 3 fan         :  6480 rpm
RFS7000#
```

2.2.40 file

▶ *Privilege / Global Config*

Syntax

```
show file (information (FILE)| systems)
```

Parameters

information (FILE)	Displays information on FILE.
systems	Lists filesystems.

Example

```
RFS7000(config)#show file systems
File Systems:

     Size(b)     Free(b)     Type  Prefix
           -           -   opaque  system:
    10485760     9912320    flash  nvram:
    20971520    19742720    flash  flash:
           -           -  network  (null)
           -           -  network  (null)
           -           -  network  sftp:
           -           -  network  http:
           -           -  network  ftp:
           -           -  network  tftp:
    20971520    19742720        -  hotspot:
RFS7000(config)#
```

2.2.41 ftp

▶ *Privilege / Global Config*

Syntax

```
show ftp
```

Parameters

None.

Example

```
RFS7000#show ftp
FTP Server: Disabled
User Name:  anonymous or ftpuser
Password:   ********
Root dir:   flash:/
RFS7000#
```

2.2.42 password-encryption

▸ *Priviledge / Global Config*

Syntax

```
show password-encryption (status)
```

Parameters

status	Displays password-encryption status.

Example

```
RFS7000#show password-encryption status
Password encryption is disabled
RFS7000#
```

2.2.43 running-config

Privilege / Global Config

Displays the contents of the configuration file for the switch, including all configured MAC and IP access lists and access groups applied to an interface.

Syntax

```
show running-config(full|include-factory)
```

Parameters

full	Full configuration.
include-factory	Includes factory defaults.

Example

```
RFS7000(config)#show running-config full
!
! configuration of RFS7000 version 1.0.0.0-228D!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
!
!
access-list 20 mark 8021p 5 any rule-precedence 10
!
spanning-tree mst config
 bridge region My Name
!
bridge spanning-tree portfast bpdu-filter
no country-code
logging console 7
snmp-server sysname RFS7000
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0x218d29df4dfde16bdec86f22cb11bc1a
snmp-server user snmpmanager v3 encrypted auth md5
0x218d29df4dfde16bdec86f22cb11bc1a
snmp-server user snmpoperator v3 encrypted auth md5
0xd9f4ec243f05174c68efb24234f16f0a
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip telnet
!
wireless
!
radius-server local
!
interface fe
 ip address dhcp
!
interface ge1
 switchport access vlan 1
!
interface ge2
switchport access vlan 1
!
interface ge3
 switchport access vlan 1
 static-channel-group 2
!
interface ge4
```

```
 switchport access vlan 1
!
interface sa2
 mtu 0
 switchport access vlan 1
 shutdown
 no multicast
!
interface tunnel27
 no ip address
!
interface vlan1
 ip address dhcp
!
interface vlan400
 no ip address
!
ip route 157.235.0.0/16 157.235.208.246
!
!
aaa authentication login default local none
line con 0
line vty 0 24
!
end

RFS7000(config)#

RFS7000(config)#show running-config include-factory
!
! configuration of RFS7000 version 1.0.0.0-228D!
version 1.0
!
service prompt crash-info
no service set command-history
no service set reboot-history
no service set upgrade-history
!
hostname RFS7000
!
banner motd Welcome to CLI!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin access  console web ssh telnet
username admin privilege  superuser
!
!
!
access-list 20 mark 8021p 5 any rule-precedence 10
!
spanning-tree mst config
 bridge region My Name
!
no management secure
ip domain-lookup
bridge spanning-tree portfast bpdu-filter
service pm max-sys-restarts 2
no service pm sys-restart
service diag period 1000
service diag enable
no country-code
redundancy group-id 1
redundancy interface-ip 0.0.0.0
redundancy mode primary
redundancy heartbeat-period 5
redundancy hold-period 15
redundancy discovery-period 30
no redundancy handle-stp enable
no redundancy enable
no logging aggregation-time
logging buffered 6
logging console 7
logging facility local7
logging host 0.0.0.0
logging host 0.0.0.0
logging host 0.0.0.0
no logging syslog
logging on
snmp-server community public  ro
snmp-server community private  rw
snmp-server location
snmp-server contact
snmp-server sysname RFS7000
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0x218d29df4dfde16bdec86f22cb11bc1a
snmp-server user snmpmanager v3 encrypted auth md5
0x218d29df4dfde16bdec86f22cb11bc1a
snmp-server user snmpoperator v3 encrypted auth md5
0xd9f4ec243f05174c68efb24234f16f0a
no snmp-server enable traps
no snmp-server enable traps snmp coldstart
no snmp-server enable traps snmp linkdown
no snmp-server enable traps snmp linkup
no snmp-server enable traps snmp authenticationFail
no snmp-server enable traps nsm dhcpIPChanged
no snmp-server enable traps redundancy memberUp
no snmp-server enable traps redundancy memberDown
no snmp-server enable traps redundancy memberMisConfigured
no snmp-server enable traps redundancy adoptionExceeded
no snmp-server enable traps redundancy grpAuthLevelChanged
no snmp-server enable traps miscellaneous lowFsSpace
no snmp-server enable traps miscellaneous processMaxRestartsReached
no snmp-server enable traps miscellaneous savedConfigModified
no snmp-server enable traps miscellaneous serverCertExpired
no snmp-server enable traps miscellaneous caCertExpired
no snmp-server enable traps wireless station associated
no snmp-server enable traps wireless station disassociated
no snmp-server enable traps wireless station deniedAssociationOnCapability
no snmp-server enable traps wireless station deniedAssociationOnShortPream
no snmp-server enable traps wireless station deniedAssociationOnSpectrum
no snmp-server enable traps wireless station deniedAssociationOnErr
..........................................................................
..........................................................................
..........................................................................
..........................................................................
..........................................................................
..........................................................................
..........................................................................
..........................................................................
RFS7000(config)#
```

2.2.44 securitymgr

▶ *Privilege / Global Config*

Syntax

```
show securitymgr(event-logs)
```

Parameters

event-logs	Displays securitymgr event logs.

Example

```
RFS7000#show securitymgr event-logs
========================
        Event Logs
========================
1> Tue Mar 13 2007 19:15:55: CORRUPT_PACKET: source vlan200: udp: Src
157.235.188.241: Dst 157.235.188.255: Src Port 137: Dst Port 137: IP TTL less
than required: traceroute
RFS7000#
```

2.2.45 sessions

▶ *Privilege / Global Config*

Syntax

```
show sessions
```

Parameters

None.

Example

```
RFS7000(config)#show sessions
SESSION   USER       LOCATION        IDLE         START TIME
   1       cli    Console           10:18m      Feb 19 13:31:42 2007
** 2       cli    xxx.xxx.xxx.xxx   00:00m      Feb 19 14:48:24 2007
RFS7000(config)#
```

2.2.46 spanning-tree

Privilege / Global Config

Use this command to display spanning tree information.

Syntax

```
show spanning-tree (mst)[config|detail|instance]
```

Parameters

mst	Displays MST information. • config – Displays configuration information. • detail – Displays detailed information. • instance – Displays instance information.

Example

```
RFS7000(config)#show spanning-tree mst detail
% Bridge up - Spanning Tree Enabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000000000000
% 1: CIST Reg Root Id 8000000000000000
% 1: CST Bridge Id 8000000000000000
% portfast bpdu-filter enabled
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off
%   sa2: Port 2005 - Id 87d5 - Role Disabled - State Discarding
%   sa2: Designated External Path Cost 0 -Internal Path Cost 0
%   sa2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   sa2: Designated Port Id 0 - CST Priority 128  -
%   sa2: CIST Root 0000000000000000
%   sa2: Regional Root 0000000000000000
%   sa2: Designated Bridge 0000000000000000
%   sa2: Message Age 0 - Max Age 0
%   sa2: CIST Hello Time 0 - Forward Delay 0
%   sa2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   sa2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   sa2: No portfast configured - Current  portfast off
%   sa2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   sa2: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   sa2: no root guard configured     - Current root guard off
%   sa2: Configured Link Type point-to-point - Current  shared
%
%   tunnel27: Port 6 - Id 8006 - Role Designated - State Forwarding
%   tunnel27: Designated External Path Cost 0 -Internal Path Cost 0
%   tunnel27: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   tunnel27: Designated Port Id 8006 - CST Priority 128  -
%   tunnel27: CIST Root 8000000000000000
%   tunnel27: Regional Root 8000000000000000
%   tunnel27: Designated Bridge 8000000000000000
%   tunnel27: Message Age 0 - Max Age 20
%   tunnel27: CIST Hello Time 2 - Forward Delay 15
%   tunnel27: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%   tunnel27: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   tunnel27: No portfast configured - Current  portfast off
%   tunnel27: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   tunnel27: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   tunnel27: no root guard configured     - Current root guard off
%   tunnel27: Configured Link Type point-to-point - Current point-to-point
%
%   ge4: Port 2004 - Id 87d4 - Role Disabled - State Discarding
%   ge4: Designated External Path Cost 0 -Internal Path Cost 0
%   ge4: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   ge4: Designated Port Id 0 - CST Priority 128  -
%   ge4: CIST Root 0000000000000000
%   ge4: Regional Root 0000000000000000
%   ge4: Designated Bridge 0000000000000000
%   ge4: Message Age 0 - Max Age 0
%   ge4: CIST Hello Time 0 - Forward Delay 0
%   ge4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge4: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   ge4: No portfast configured - Current  portfast off
%   ge4: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge4: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   ge4: no root guard configured     - Current root guard off
%   ge4: Configured Link Type point-to-point - Current  shared
%
%   ge2: Port 2002 - Id 87d2 - Role Disabled - State Discarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 0
%   ge2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   ge2: Designated Port Id 0 - CST Priority 128  -
%   ge2: CIST Root 0000000000000000
%   ge2: Regional Root 0000000000000000
%   ge2: Designated Bridge 0000000000000000
%   ge2: Message Age 0 - Max Age 0
%   ge2: CIST Hello Time 0 - Forward Delay 0
%   ge2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   ge2: No portfast configured - Current  portfast off
%   ge2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge2: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current  shared
%
%   ge1: Port 2001 - Id 87d1 - Role Disabled - State Discarding
%   ge1: Designated External Path Cost 0 -Internal Path Cost 0
%   ge1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   ge1: Designated Port Id 0 - CST Priority 128  -
%   ge1: CIST Root 0000000000000000
%   ge1: Regional Root 0000000000000000
%   ge1: Designated Bridge 0000000000000000
%   ge1: Message Age 0 - Max Age 0
%   ge1: CIST Hello Time 0 - Forward Delay 0
%   ge1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge1: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   ge1: No portfast configured - Current  portfast off
%   ge1: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge1: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   ge1: no root guard configured     - Current root guard off
%   ge1: Configured Link Type point-to-point - Current  shared
%
RFS7000(config)#

RFS7000(config)#show spanning-tree mst instance
% Bridge up - Spanning Tree Enabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000000000000
% 1: CIST Reg Root Id 8000000000000000
% 1: CST Bridge Id 8000000000000000
% portfast bpdu-filter enabled
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off
%   sa2: Port 2005 - Id 87d5 - Role Disabled - State Discarding
%   sa2: Designated External Path Cost 0 -Internal Path Cost 0
%   sa2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   sa2: Designated Port Id 0 - CST Priority 128  -
%   sa2: CIST Root 0000000000000000
%   sa2: Regional Root 0000000000000000
%   sa2: Designated Bridge 0000000000000000
%   sa2: Message Age 0 - Max Age 0
%   sa2: CIST Hello Time 0 - Forward Delay 0
%   sa2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   sa2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   sa2: No portfast configured - Current  portfast off
%   sa2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   sa2: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   sa2: no root guard configured     - Current root guard off
%   sa2: Configured Link Type point-to-point - Current  shared
%
%   tunnel27: Port 6 - Id 8006 - Role Designated - State Forwarding
%   tunnel27: Designated External Path Cost 0 -Internal Path Cost 0
%   tunnel27: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   tunnel27: Designated Port Id 8006 - CST Priority 128  -
%   tunnel27: CIST Root 8000000000000000
%   tunnel27: Regional Root 8000000000000000
%   tunnel27: Designated Bridge 8000000000000000
%   tunnel27: Message Age 0 - Max Age 20
%   tunnel27: CIST Hello Time 2 - Forward Delay 15
%   tunnel27: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1
%   tunnel27: Version Multiple Spanning Tree Protocol - Received None - Send MSTP
%   tunnel27: No portfast configured - Current  portfast off
tunnel27: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   tunnel27: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   tunnel27: no root guard configured     - Current root guard off
%   tunnel27: Configured Link Type point-to-point - Current point-to-point
%
%   ge4: Port 2004 - Id 87d4 - Role Disabled - State Discarding
%   ge4: Designated External Path Cost 0 -Internal Path Cost 0
%   ge4: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   ge4: Designated Port Id 0 - CST Priority 128  -
%   ge4: CIST Root 0000000000000000
%   ge4: Regional Root 0000000000000000
%   ge4: Designated Bridge 0000000000000000
%   ge4: Message Age 0 - Max Age 0
%   ge4: CIST Hello Time 0 - Forward Delay 0
%   ge4: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge4: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   ge4: No portfast configured - Current  portfast off
%   ge4: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge4: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   ge4: no root guard configured     - Current root guard off
%   ge4: Configured Link Type point-to-point - Current  shared
%
%   ge2: Port 2002 - Id 87d2 - Role Disabled - State Discarding
%   ge2: Designated External Path Cost 0 -Internal Path Cost 0
%   ge2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   ge2: Designated Port Id 0 - CST Priority 128  -
%   ge2: CIST Root 0000000000000000
%   ge2: Regional Root 0000000000000000
%   ge2: Designated Bridge 0000000000000000
%   ge2: Message Age 0 - Max Age 0
%   ge2: CIST Hello Time 0 - Forward Delay 0
%   ge2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   ge2: No portfast configured - Current  portfast off
%   ge2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge2: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   ge2: no root guard configured     - Current root guard off
%   ge2: Configured Link Type point-to-point - Current  shared
%
%   ge1: Port 2001 - Id 87d1 - Role Disabled - State Discarding
%   ge1: Designated External Path Cost 0 -Internal Path Cost 0
%   ge1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   ge1: Designated Port Id 0 - CST Priority 128  -
%   ge1: CIST Root 0000000000000000
%   ge1: Regional Root 0000000000000000
%   ge1: Designated Bridge 0000000000000000
%   ge1: Message Age 0 - Max Age 0
%   ge1: CIST Hello Time 0 - Forward Delay 0
%   ge1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%   ge1: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   ge1: No portfast configured - Current  portfast off
%   ge1: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   ge1: portfast bpdu-filter default  - Current portfast bpdu-filter on
%   ge1: no root guard configured     - Current root guard off
%   ge1: Configured Link Type point-to-point - Current  shared
%
RFS7000(config)#
```

2.2.47 startup-config

▶ *Privilege / Global Config*

Syntax

```
show startup-config
```

Parameters

None.

Example

```
RFS7000#show startup-config
!
! configuration of RFS7000 version 1.0.0.0-228D!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
!
!
!
spanning-tree mst config
 bridge region My Name
!
no country-code
logging console 7
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0x218d29df4dfde16bdec86f22cb11bc1a
snmp-server user snmpmanager v3 encrypted auth md5
0x218d29df4dfde16bdec86f22cb11bc1a
snmp-server user snmpoperator v3 encrypted auth md5
0xd9f4ec243f05174c68efb24234f16f0a
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
ip telnet
!
wireless
!
radius-server local
!
interface fe
 ip address dhcp
!
interface ge1
 switchport access vlan 1
!
interface ge2
 switchport access vlan 1
!
interface ge3
..................................
RFS7000#
```

2.2.48 static-channel-group

▶ *Privilege / Global Config*

Use the `show static-channel-group` privileged EXEC command to display configured static channel groups.

Syntax

```
show static-channel-group
```

Parameters

None.

Example

```
RFS7000(config)#show static-channel-group
% Static Aggregator: sa2
% Member:
   ge3
RFS7000(config)#
```

2.2.49 upgrade-status

▶ *Privilege / Global Config*

Syntax

```
show upgrade-status(detail)
```

Parameters

detail	Last image upgrade log.

Example

```
RFS7000#show upgrade-status detail
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Tue Aug 29 18:32:17 2006
--------------------------------------------------------
var2 is 10 percent full
/tmp is 5 percent full
Free Memory 151944 kB
FWU invoked via Linux shell
Running from partition /dev/hda6, partition to update is /dev/hda5
Reading image file header
Removing other partition
Added 3.0.0.0-180B *
Making file system
Extracting files (this can take some time).
Version of firmware update file is 3.0.0.0-200B
Creating LILO files
Running LILO
Added 3.0.0.0-180B *
Added 3.0.0.0-200B
Successful
RFS7000RFS7000#
```

2.2.50 wlan-acl

▶ *Privilege / Global Config*

Syntax

```
show wlan-acl [<1-256>|all]
```

<1-256>	Displays ACLs attached to the specified WLAN ID.
all	Displays ACLs attached to WLAN port.

Example

```
RFS7000(config)#show wlan-acl 102
WLAN port: 102
  Inbound IP Access List : 110
  Inbound MAC Access List :

  Outbound IP Access List:
  Outbound MAC Access List :
RFS7000(config)#
```

☑ NOTE The above example applies ACL 110 to a WLAN index 102 in inbound direction.

3

User Exec Commands

Logging in to the switch places you within the USER EXEC command mode. Typically, a log-in requires a user name and a password. You have three attempts to enter a password correctly before a connection attempt is refused.The USER EXEC commands available at the user level are a subset of those available at the privileged level. In general, the user EXEC commands allow you to connect to remote devices, perform basic tests and list system information.

To list available USER EXEC commands, use the **?** at the command prompt. The USER EXEC mode prompt consists of the device host name followed by an angle bracket (**>**). The default host name is generally RFS7000. Use the hostname GLOBAL CONFIG command to change the hostname.

3.1 User Exec Commands

Table 3.1 summarizes User Exec commands.

Table 3.1 User Exec commands Summary

Command	Description	Ref.
clear	Resets the command to previous configuration.	page 3-3
clrscr	Clears the display screen.	page 2-3
cluster-cli	Cluster context.	page 3-4
debug	Debugging functions.	page 3-5
disable	Turns off the privileged mode command.	page 3-6
enable	Turns on the privileged mode command.	page 3-7
exit	Ends the current mode and moves down to the previous mode.	page 2-10
help	Description of the interactive help system.	page 2-11
logout	Exits the EXEC mode.	page 3-8
no	Negates a command or sets its defaults.	page 2-12
page	Toggle paging.	page 3-9
quit	Exits the current mode and moves down to the previous mode.	page 3-10
service	Service commands.	page 2-13
show	Shows running system information	page 3-11
terminal	Shows running system information.	page 2-24

3.1.1 clear

▶ *User Exec Commands*

Use this command to reset the command to previous configuration.

Syntax

```
clear (mobility|spanning-tree)
clear mobility(event-log|mobile-unit|peer-statistics)
clear mobility event-log(mobile-unit|peer)

clear spanning-tree (detected)(protocols)(bridge|interface)
```

Parameters

mobility	Clears mobility attributes.
event-log	Clears mobility attirbutes from event log of: • mobile-unit – Mobile unit event-logs. • peer – Peer event-logs.
mobile-unit	Clears mobile unit information.
peer-statistics	Clears mobility peer statistcs.
spanning-tree	Clears spanning tree attributes.
detected	Clears spanning tree for the detected spanning tree.
protocols	Clears spanning tree protocols.
bridge	Clears spanning tree bridge.
interface <name>	Clears spanning tree interface name.

Example

```
RFS7000>clear mobility event-log mobile-unit
RFS7000>

RFS7000>clear mobility event-log peer
RFS7000>

RFS7000>clear mobility mobile-unit all
RFS7000>

RFS7000>clear mobility mobile-unit home-database
RFS7000>

RFS7000>clear spanning-tree detected protocols bridge
RFS7000>

RFS7000>clear spanning-tree detected protocols interface Nexus
RFS7000>
```

3.1.2 cluster-cli

▶ *User Exec Commands*

Use this command to cluster all the CLI pertaining to the context it appears in. This feature is useful to configure each switch in the cluster by logging in to one switch which participates in the cluster. This eliminates the administrator time and effort N-1 times if there are N switches in the cluster.

A new context called *redundancy* is created to support cluster-cli. Any commands executed under this context are also executed to all members of the cluster.

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables cluster context.

Example

```
RFS7000(config)#show redundancy-members

Member ID                      : 192.168.100.1
Member State                   : Peer Seen
Member First Seen              : Mar 15 16:24:54 2008
Member Last  Seen              : Mar 15 16:25:00 2008
Number of HB sent              : 38044
Number of HB received          : 3
Number of Update sent          : 0
Number of Update received      : 0
Member Standby Mode            : Primary
Member AP adoption count       : 0
Member Installed License Count: 0
Member Radio portal Count      : 0
Member Associated MU Count     : 0
Member Rogue AP detected Count: 0
Member Self Healing AP Count   : 0
Member Switch Adopt Capacity   : 0
Member Running Image Version   :

RFS7000(config)#


RFS7000:cluster-cli#show version
*** START: Response from member: 172.20.15.18 ****

RFS7000 version 1.0.0.0-261X
Copyright © 2006 Symbol Technologies, Inc.
Booted from primary.
Switch uptime is 7 days, 4 hours 28 minutes

*** END: Response from member: 172.20.15.18 ****

RFS7000 version 1.0.0.0-262X
Copyright © 2006 Symbol Technologies, Inc.
Booted from primary.
Switch uptime is 7 days, 4 hours 28 minutes

RFS7000:cluster-cli#
```

3.1.3 debug

▶ User Exec Commands

Use this command to debug the switch.

Syntax

```
debug (certmgr(all|err|info)|
       ip(https|ssh)|
        mobility(cc|error|forwarding|mu|packet|peer|system)|
        mstp(all|cli|packet(rx|tx)|protocol (detail)|timer (detail))
```

Parameters

certmgr	Certificate manager debugging messages.
ip ( )	Internet Protocol (IP). • https – Secure HTTP (HTTPS) server. • ssh – Secured SHell (SSH) server.
mobility ( )	L3 Mobility • cc – ccserver events. • error – Error. • forwarding – Dataplane forwarding. • mu – MU events and state changes. • packet – Control packets. • peer – Peer establishment. • system – System events.
mstp ( )	Turn on/off mstp debugging messages. • all – Debugs the entire MSTP. • cli – Debugs all the MSTP CLI commands. • packet – Debugs MSTP packets. • protocol – Debugs MSTP protocols. • timer – Debugs the MSTP timer.

Example

```
RFS7000>debug certmgr all
RFS7000>

RFS7000>debug certmgr error
RFS7000>

RFS7000>debug certmgr info
RFS7000>

RFS7000>debug mstp all
RFS7000>

RFS7000>debug mstp cli
RFS7000>
```

3.1.4 disable

▶ *User Exec Commands*

Enable the PRIV mode to use this command. Then, use the `disable` command to exit the PRIV mode.

Syntax

```
disable
```

Parameters

None.

Example

```
RFS7000>disable
RFS7000>
```

3.1.5 enable

▸ *User Exec Commands*

Use this command to enter the PRIV mode.

Syntax

```
enable
```

Parameters

None.

Example

```
RFS7000>enable
```

3.1.6 logout

▶ *User Exec Commands*

Use this command instead of `exit` command to exit the EXEC mode.

Syntax

```
logout
```

Parameters

None.

Example

```
The RFS7000 Series Switch logs off on execution of this command.
```

3.1.7 page

▶ *User Exec Commands*

Use this command to toggle paging. Enabling this command displays the CLI command output page by page, instead of running the entire output at once.

Syntax

```
page
```

Parameters

None.

Example

```
RFS7000>page ?
  <cr>

RFS7000>page

RFS7000>enable
RFS7000#show running-config
!
! configuration of RFS7000 version 1.0.0.0-280D!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
!
!
access-list 110 permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
access-list 110 permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
access-list 110 permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
!
spanning-tree mst config
 name My Na
```

3.1.8 quit

▶ *User Exec Commands*

Use this command to exit the current mode, and move back down to the previous mode.

Syntax

```
quit
```

Parameters

None.

Example

The switch logs off upon execution of this command.

3.1.9 show

▶ *User Exec Commands*

Use this command to exit the current mode and go down to previous mode.

Syntax

```
show
```

Parameters

autoinstall	Displays the autoinstall configuration.
banner	Displays the “Message of the Day Login” banner.
commands	Displays command lists.
debugging	Displays debugging information outputs.
history	Displays the session command history.
interfaces	Displays interface status.
ip	Displays the Internet Protocol (IP).
ldap	Displays LDAP server details.
licenses	Displays any installed licenses details.
logging	Displays logging configuration and buffer information.
mac	Displays MAC access-list assignment.
management	Displays L3 Managment Interface name.
mobility	Displays mobility parameters.
ntp	Displays the network time protocol.
privilege	Displaysthe current privilege level.
radius	Displays RADIUS configuration commands.
redundancy-group	Displays redundancy group parameters.
redundancy-history	Displays the state transition history of the switch.
redundancy-members	Displays redundancy group members in detail.
snmp	Displays SNMP engine parameters.
snmp-server	Displays SNMP Server parameters.
spanning-tree	Displays spanning-tree information.
static-channel-group	Displays static channel group membership.
terminal	Displays terminal configuration parameters.
timezone	Displays timezone.
users	Displays information about terminal lines.

version	Displays the software and hardware version.
wireless	Displays wireless configuration commands.
wlan-acl	Displays WLAN based ACL information.

Example

```
RFS7000>show autoinstall
feature    enabled      URL
config       yes        --not-set--
cluster cfg  yes        --not-set--
image        yes        --not-set--
expected image version  --not-set--
RFS7000>

RFS7000>show commands
  clear mobility event-log (mobile-unit|peer)
  clear mobility event-log (mobile-unit|peer)
  clear mobility mobile-unit (AA-BB-CC-DD-EE-FF|home-database|foreign-
database|all)
  clear mobility mobile-unit (AA-BB-CC-DD-EE-FF|home-database|foreign-
database|all)
  clear mobility mobile-unit (AA-BB-CC-DD-EE-FF|home-database|foreign-
database|all)
  clear mobility mobile-unit (AA-BB-CC-DD-EE-FF|home-database|foreign-
database|all)
  clear mobility peer-statistics (A.B.C.D|)
  clear mobility peer-statistics (A.B.C.D|)
  clear spanning-tree detected protocols bridge
  clear spanning-tree detected protocols interface INTERFACE
  clrscr
  cluster-cli enable
  debug certmgr ( error|info|all )
  debug certmgr ( error|info|all )
  debug certmgr ( error|info|all )
  debug ip https
  debug ip ssh
...................................................................
...................................................................
RFS7000>

RFS7000>show history
   1 admin
   2 show autoinstall
   3 show banner
   4 clrscr
   5 show commands
   6 clrscr
   7 show debugging
   8 show history
RFS7000>

RFS7000>show interfaces
Interface fe
  Hardware Type Ethernet, Interface Mode Layer 3, address is 00-15-70-37-fc-93
  index=1, metric=1, mtu=1500, (PAL-IF)  <UP,BROADCAST,RUNNING,MULTICAST>
  Speed: Admin Auto, Operational 100M, Maximum 100M
  Duplex: Admin Auto, Operational Full
  Active Medium: Copper
  inet 157.235.208.122/24 broadcast 157.235.208.255
    input packets 138225, bytes 39061067, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 4642, bytes 424662, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
Interface vlan1
  Hardware Type VLAN, Interface Mode Layer 3, address is 00-15-70-37-fc-8f
  index=5, metric=1, mtu=1500, (PAL-IF)  <UP,BROADCAST,RUNNING,MULTICAST>
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 1375, bytes 475750, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
Interface ge1
  Hardware Type Ethernet, Interface Mode Layer 2, address is 00-15-70-37-fc-8f
  index=2001, metric=1, mtu=1500, (HAL-IF)  <UP,BROADCAST,MULTICAST>
  Speed: Admin Auto, Operational Unknown, Maximum 1G
  Duplex: Admin Auto, Operational Unknown
  Active Medium: Unknown
  Switchport Settings: Mode: Access, Access Vlan: 1
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
Interface ge2
  Hardware Type Ethernet, Interface Mode Layer 2, address is 00-15-70-37-fc-90
  index=2002, metric=1, mtu=1500, (HAL-IF)  <UP,BROADCAST,MULTICAST>
  Speed: Admin Auto, Operational Unknown, Maximum 1G
  Duplex: Admin Auto, Operational Unknown
  Active Medium: Unknown
  Switchport Settings: Mode: Access, Access Vlan: 1
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
Interface ge3
  Hardware Type Ethernet, Interface Mode Layer 2, address is 00-15-70-37-fc-91
  index=2003, metric=1, mtu=1500, (HAL-IF)  <UP,BROADCAST,MULTICAST>
  Speed: Admin Auto, Operational Unknown, Maximum 1G
  Duplex: Admin Auto, Operational Unknown
  Active Medium: Unknown
  Switchport Settings: Mode: Access, Access Vlan: 1
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
Interface ge4
  Hardware Type Ethernet, Interface Mode Layer 2, address is 00-15-70-37-fc-92
  index=2004, metric=1, mtu=1500, (HAL-IF)  <UP,BROADCAST,MULTICAST>
  Speed: Admin Auto, Operational Unknown, Maximum 1G
  Duplex: Admin Auto, Operational Unknown
  Active Medium: Unknown
  Switchport Settings: Mode: Access, Access Vlan: 1
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
RFS7000>
```

RFS7000>show **logging**

```
Logging module: enabled
    Aggregation time: disabled
    Console logging: level debugging
    Monitor logging: disabled
    Buffered logging: level informational
    Syslog logging: disabled
```

```
Log Buffer (3552 bytes):

Feb 16 18:38:03 2007: %IMI-5-USERAUTHSUCCESS: User 'admin' logged in with role of
' superuser' from auth source 'local'

Feb 16 18:37:58 2007: %AUTH-6-INFO: login[20553]: root login  on `pts/0' from
`157.235.206.225'

Feb 16 18:14:32 2007: %USER-0-EMERG: WIOS_CCSERVER[1018]:  ccsrvr is creating
core on users request

Feb 16 18:14:25 2007: %DIAG-6-FREERAMDISK: Free /var file system space, 0.0% is
less than limit 10.0%

Feb 16 18:14:15 2007: %USER-0-EMERG: WIOS_CCSERVER[1018]:  ccsrvr is creating
core on users
request..........................................................................
.................................................................................
.................................................................................
.....................................................
RFS7000>

RFS7000>show management
Mgmt Interface: vlan1
Management access permitted via any vlan interface
RFS7000>
```

4

Privileged Exec Commands

Most PRIV EXEC mode commands set operating parameters. Privileged-level access must be password protected to prevent unauthorized use. The PRIV EXEC command set includes those commands contained in USER EXEC mode. The PRIV EXEC mode also provides access to configuration modes using the configure command, and includes advanced testing commands.

The PRIV EXEC mode prompt consists of the host name of the device, followed by a pound sign (**#**). To access PRIV EXEC mode, enter the following command at the prompt:

```
RFS7000#enable
```

PRIV EXEC mode is sometimes referred to as **enable mode**, because the `enable` command is used to enter the mode.

If a password has been configured on the system, you are prompted to enter the password before allowed access to privileged EXEC mode. The password is not displayed on the screen and is case sensitive. If an enable password has not been set, the PRIV EXEC mode can be accessed only from the router console (terminal connected to the console port). Use enable secret or enable password.

4.1 Priv Exec Command

Table 4.1 summarizes the Priv Exec commands.

Table 4.1 Priv Exec Command Summary

Command	Description	Ref.
acknowledge	Acknowledges alarms.	page 4-4
archive	Manages archive files.	page 4-5
cd	Changes the current directory.	page 4-6
change-passwd	Changes the password of the logged in user.	page 4-7
clear	Reset function.	page 4-8
clock	Configures the software system clock.	page 4-10
clrscr	Clears the displayed screen.	page 2-3
cluster-cli	Cluster context.	page 4-11
configure	Enters the configuration mode.	page 4-12
copy	Copies from one file to another.	page 4-13
debug	Debugging functions.	page 4-14
delete	Deletes a specified file from the system.	page 4-16
diff	Displays the differences between two files.	page 4-17
dir	Lists files on a file system.	page 4-18
disable	Turns off a privileged mode command.	page 4-19
edit	Edits a text file.	page 4-20
enable	Turns on the privileged mode command.	page 4-21
erase	Erases a filesystem.	page 4-22
exit	Ends the current mode and moves down to the previous mode.	page 2-10
help	Description of the interactive help system.	page 2-11
kill	Kills the specified session.	page 4-23
logout	Exits the EXEC mode.	page 4-24
mkdir	Creates a directory.	page 4-25
more	Displays the contents of a file.	page 4-26
no	Negates a command or set its defaults.	page 2-12
page	Toggles the paging functionality.	page 4-27

Command	Description	Ref.
ping	Sends an ICMP echo message.	page 4-28
pwd	Displays the current directory.	page 4-29
quit	Exits the current mode and moves down to the previous mode.	page 4-30
reload	Halts the switch and performs a warm reboot.	page 4-31
rename	Renames a file.	page 4-32
rmdir	Deletes a directory.	page 4-33
service	Service commands.	page 2-13
show	Shows system information.	page 4-34
telnet	Opens a telnet connection.	page 4-37
terminal	Shows running system information.	page 2-24
traceroute	Traces a route to a destination.	page 4-38
upgrade	Upgrades the software image.	page 4-39
upgrade-abort	Aborts the upgrade process.	page 4-41
write	Writes the running configuration to memory or terminal.	page 4-42

4.1.1 acknowledge

- *Priv Exec Command*

Use this command to acknowledge alarms.

Syntax

```
acknowledge alarm-log [<1-65535> | all]
```

Parameters

alarm-log	Acknowledge an alarm. • <1-65535> – Acknowledges specific alarm id. • all – Acknowledges all alarms.

Example

```
RFS7000#acknowledge alarm-log all
No corresponding record found in the Alarm Log.

RFS7000#acknowledge alarm-log 200
No corresponding record found in the Alarm Log.
RFS7000#
```

4.1.2 archive

- *Priv Exec Command*

Use this command to manage archive files.

Syntax

```
archive tar /table [FILE|URL]
archive tar /create [FILE|URL] FILE
archive tar /xtract [FILE|URL] DIR
```

Parameters

tar	Manipulates (creates, lists or extracts) a tar file.
/table	Lists files in a tar file.
/create	Creates a tar file.
/xtract	Extracts files from a tar file.
FILE	Tar filename.
URL	Tar file URL.

Example

How to zip the folder flash:/log/?

```
RFS7000#archive tar /create flash:/out.tar flash:/log/
tar: Removing leading '/' from member names
flash/log/
flash/log/snmpd.log
flash/log/messages.log
flash/log/startup.log
flash/log/radius/
RFS7000#dir flash:/
```

Viewing the output tar file?

```
Directory of flash:/
  drwx   1024      Thu Aug 17 08:25:50 2006   hotspot
  drwx   120       Fri Sep  8 12:27:20 2006   log
  drwx   1024      Thu Sep  7 16:23:34 2006   crashinfo
  drwx   1024      Wed Aug 23 15:30:19 2006   backup
  -rw-   173056    Fri Sep  8 14:39:48 2006   out.tar
```

Which files are tared?

```
RFS7000#archive tar /table flash:/out.tar
drwxrwxrwt 0/600         0 2006-09-08 12:27:20 flash/log
-rw-r--r-- 0/0         381 2006-09-08 12:27:28 flash/log/snmpd.log
-rw-r--r-- 0/0      151327 2006-09-08 14:37:26 flash/log/messages.log
-rw-r--r-- 0/0       17318 2006-09-08 12:27:29 flash/log/startup.log
drwxrwxrwt 0/600         0 2006-09-08 12:27:14 flash/log/radius
```

Untar fails..?

```
RFS7000#archive tar /xtract flash:/out.tar flash:/out/
tar: flash:/out.tar: No such file or directory
```

4.1.3 cd

▶ *Priv Exec Command*

Use this command to change the current directory.

Syntax

```
cd [DIR|]
```

Parameters

DIR	Changes the current directory to DIR.

Example

```
RFS7000#cd
nvram:/   system:/  flash:/
RFS7000#cd flash:/?
  DIR  Change current directory to DIR
RFS7000#cd flash:/
flash:/backup/     flash:/crashinfo/  flash:/hotspot/    flash:/log/
flash:/out/
RFS7000#cd flash:/log/?
  DIR  Change current directory to DIR
RFS7000#cd flash:/log/
RFS7000#pwd
flash:/log/
RFS7000#
```

4.1.4 change-passwd

▶ *Priv Exec Command*

Use this command to change the password of the logged in user.

Syntax

```
change-passwd
```

Parameters

None.

Usage Guidelines

A password must be between 8 to 32 characters in length. For safety reasons, the console does not display the user entered key words (refer example) for the `old password` and `new password` fields.

Ensure the console displays the password successfully changed message.

☑ **NOTE** The console, by default, does not display any user entered keyword for the old pasword and new password fields.

Leaving the `old password` and `new password` field empty displays the following error message:

```
Error: Invalid password length. It should be between 8 - 32
characters.
```

Example

```
RFS7000#change-passwd
Enter old password:
Enter new password:
Password for user 'admin' changed successfully
RFS7000#
```

4.1.5 clear

▶ *Priv Exec Command*

Use this command to reset the current context.

Syntax

```
clear [alarm-log|arp-cache|ip|logging|mac|mobility|spanning-tree]

clear alarm-log (<1-65535>|acknowledge|all|new)

clear ip(dhcp(binding)[*|A.B.C.D])

clear mac (address-table) [dynamic|multicast|static]
                          [address|bridge <1-32>|interface|vlan <1-4094>]

clear mobility [event-log (mobile-unit|peer)|
mobile-unit (<MAC Address >|all|foreign-database|home-database)|
peer-statistics <Peer IP Address>]

clear spanning-tree (detected)[bridge|interface(name)]
```

Parameters

alarm-log	Clears the alarm-log. • <1-65535> – Clear specific alarm id. • acknowledge – Clear acknowledged alarms. • all – Clear all alarms. • new – Clear new alarms.
arp-cache	Clears the Arp cache.
ip (dhcp (binding) [*|A.B.C.D])	Clears the Internet Protocol (IP) of DHCP. • dhcp – DHCP Server configuration. • *binding* – DHCP Address bindings. • *** – Clear all bindings. • *A.B.C.D* – Clear a specific binding.
logging	Modifies message logging facilities.
mac (address-table) [dynamic|multicast|static] [*address*|*bridge <1-32>*| *interface*|*vlan*]	Clears layer 2 MAC entries. • address-table – Clears all Entries in the forwarding database. • dynamic – Clears all dynamic entries. • multicast – Clears all multicast entries. • static – Clears all entries configured through management. • *address* – Clears the specified MAC Addresss/ Interface Name/ VLAN ID (1-4094). • *bridge* <1-32> – Bridge group for bridging. • *interface* – Clears MAC address for the specified VLAN. • *vlan* – Clears MAC address for the specified interface.

mobility [event-log (mobile-unit|peer)| mobile-unit (<MAC Address >|all|foreign-database|home-database)| peer-statistics <Peer IP Address>]	Clear mobility attributes. • event-log – Clears all event logs. • *mobile-unit* – Mobile unit event logs. • *peer* – Peer event logs. • mobile-unit – Clears a mobile unit. • *AA-BB-CC-DD-EE-FF* – MAC address of the mobile unit. • *all* – All mobile units (Home and Foreign). • *foreign-database* – Mobile units present in the foreign mobile unit database. • *home-database* – Mobile units present in the home mobile unit database. • peer-statistics – Clears mobility peer statistcs. • *A.B.C.D* – IP address of Peer.
spanning-tree (detected) [bridge|interface(name)]	Clears spanning tree attributes.

Example

```
RFS7000#clear spanning-tree detected protocols bridge
RFS7000#

RFS7000#clear alarm-log new
RFS7000#

RFS7000#clear alarm-log acknowledged
RFS7000#

RFS7000#clear arp-cache
RFS7000#

RFS7000#clear logging
RFS7000#

RFS7000#clear mobility event-log peer
RFS7000#

RFS7000#clear ip dhcp binding *
RFS7000#
```

4.1.6 clock

Priv Exec Command

Use this command to configure the software system clock.

Syntax

```
clock set HH:MM:SS [1-31] MONTH [1993-2035]
```

Parameters

set	Sets the system date and time.

Example

```
RFS7000#clock set 15:10:30 08 Sep 2006
RFS7000#show clock
Sep 08 15:10:31 UTC 2006
```

4.1.7 cluster-cli

▶ *Priv Exec Command*

Use this command to cluster all the CLI pertaining to the context it appears in. This feature is useful to configure each switch in the cluster by logging in to one participating switch. This eliminates administrator time and effort, as one switch configuration can represent the entire cluster.

A new context called *redundancy* is available to support the cluster-cli. Any commands executed under this context are also executed each cluster member.

Syntax

```
cluster-cli enable
```

Parameters

enable	Enables the cluster context.

Example

```
RFS7000(config)#show redundancy-members

Member ID                     : 192.168.100.1
Member State                  : Peer Seen
Member First Seen             : Mar 15 16:24:54 2008
Member Last  Seen             : Mar 15 16:25:00 2008
Number of HB sent             : 38044
Number of HB received         : 3
Number of Update sent         : 0
Number of Update received     : 0
Member Standby Mode           : Primary
Member AP adoption count      : 0
Member Installed License Count: 0
Member Radio portal Count     : 0
Member Associated MU Count    : 0
Member Rogue AP detected Count: 0
Member Self Healing AP Count  : 0
Member Switch Adopt Capacity  : 0
Member Running Image Version  :

RFS7000(config)#

RFS7000:cluster-cli#show version
*** START: Response from member: 172.20.15.18 ****

RFS7000 version 1.0.0.0-261X
Copyright © 2006 Symbol Technologies, Inc.
Booted from primary.
Switch uptime is 7 days, 4 hours 28 minutes

*** END: Response from member: 172.20.15.18 ****

RFS7000 version 1.0.0.0-262X
Copyright © 2006 Symbol Technologies, Inc.
Booted from primary.
Switch uptime is 7 days, 4 hours 28 minutes

RFS7000:cluster-cli#
```

4.1.8 configure

▶ *Priv Exec Command*

Use this command to move into the configuration mode.

Syntax

```
configure terminal
```

Parameters

terminal	Configures from the terminal.

Example

```
RFS7000#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
RFS7000(config)#
```

4.1.9 copy

▶ *Priv Exec Command*

Use this command to copy any file (config,log,txt ...etc) from any location to the switch and vice-versa.

NOTE Copying a new config file onto an exisitng running-config file merges it with the existing running-config on the switch. Both, the exisitng running-config and the new config file parameters are applied as the current running-config of the switch.

Copying a new config file onto a start-up config files replaces the exisitng start-up config file with the parameters of the new config file. It is always better to erase the existing start-up config file from the switch and then copy the new config file to the startup config.

Syntax

```
copy (FILE|URL) (FILE|URL)
```

Parameters

FILE	Target file from which to copy.
URL	The targer URL from which to copy.

Example

Transfering file snmpd.log to remote tftp server?

```
RFS7000#copy flash:/log/snmpd.log
tftp://157.235.208.105:/snmpd.log
```

Accessing running-config file from remote tftp server into switchrunning-config?

```
RFS7000#copy tftp://157.235.208.105:/running-
config running-config
```

4.1.10 debug

▸ *Priv Exec Command*

Use this command for debugging purposes. This command is also used to debug various features.

Syntax

```
debug all
debug cc [access-port|all|alt|ap-detect|capwap|cluster|
          config|dot11|eap|ids|kerberos|l3-mob|media|mobile-unit|radio|
           radius|self-heal|snmp|system|wips|wisp]
debug ccstats <CCStats Module>
debug certmgr [all|error|info]
debug dhcpsvr [all|error|info]
debug imi [all|cli-client|cli-server|errors|init|ntp]
debug ip [https|ssh]
debug logging [all|errors|monitor|subagent]
debug mgmt [all|cgi|err|sys]
debug mobility [all|cc|error|forwarding|mu|packet|peer|system]
debug mstp [all|cli|packet|protocol|timer]
debug nsm [all|events|kernel|packet]
debug pktdrvr [rate-limit|skip-packet-filter]
debug pm [all|errors|heartbeats|init|proc|shutdown|subagent|sys]
debug radius [all|err|info|warn]
debug redundancy [all|ccmsg|config|errors|general|heartbeats|
                init|packets|proc|shutdown|states|subagent|timer|warnings]
debug securitymgr [all|debug|error|ikeerror|pmdebug|pmerror]
```

Parameters

all	Enables debugging functionalities.
cc	Cellcontroller (wireless) debugging messages.
ccstats	Cellcontroller (wireless) debugging messages.
certmgr	Certificate manager debugging messages.
dhcpsvr	DHCP conf server debugging messages.
imi	Integrated management interface.
ip	Internet protocol (IP).
logging	Modifies message logging facilities.
mgmt	Management daemon.
mobility	L3 mobility.
mstp	Multiple spanning tree protocol.
nsm	Network Service Module (NSM).
pktdrvr	Pktdrvr (kernel wireless) debugging messages.
pm	Process monitor.
radius	RADIUS server debugging messages.
redundancy	Redundancy Protocol debugging messages.
securitymgr	Security manager debugging messages.

Example

```
RFS7000#debug ?
  all          Enable all debugging
  cc           Cellcontroller (wireless) debugging messages
  ccstats      Cellcontroller (wireless) debugging messages
  certmgr      Certificate Manager Debugging Messages
  dhcpsvr      DHCP Conf Server Debugging Messages
  imi          Integrated Management Interface
  ip           Internet Protocol (IP)
  logging      Modify message logging facilities
  mgmt         Mgmt daemon
  mobility     L3 Mobility
  mstp         Multiple Spanning Tree Protocol (MSTP)
  nsm          Network Service Module (NSM)
  pktdrvr      Pktdrvr (kernel wireless) debugging messages
  pm           Process Monitor
  radius       RADIUS server debugging messages
  redundancy   Redundancy Protocol debugging messages
  securitymgr  Security Manager Debugging Messages

RFS7000#debug
```

4.1.11 delete

▸ *Priv Exec Command*

Use this command to delete the specified file from the system.

Syntax

```
delete ({/force|/recursive}|) .FILE
```

Parameters

/force	Forces deletion without a prompt.
/recursive	Performs a recursive delete.
FILE	Specifies the filename(s) to be deleted.

Example

```
RFS7000#delete flash:/out.tar flash:/out.tar.gz
Delete flash:/out.tar [y/n]? y
Delete flash:/out.tar.gz [y/n]? y

RFS7000#delete /force flash:/tmp.txt
RFS7000#

RFS7000#delete /recursive flash:/backup/
Delete flash:/backup//fileMgmt_350_180B.core

[y/n]? y
Delete

flash:/backup//fileMgmt_350_18212X.core_bk

[y/n]? n
Delete flash:/backup//imish_1087_18381X.core.gz

[y/n]? n
RFS7000#
```

4.1.12 diff

▶ *Priv Exec Command*

Use this command to view the difference between two files.

Syntax

```
diff (FILE|URL) (FILE|URL)
```

Parameters

FILE	Displays the differences between FILE.
URL	Displays the differences between URL.

Example

```
RFS7000#diff startup-config running-config
--- startup-config
+++ running-config
@@ -89,7 +89,7 @@
  mobility peer 157.235.208.16
  wlan 1 enable
  wlan 1 ssid wlan123
- wlan 1 encryption-type wep128
+ wlan 1 encryption-type tkip
  wlan 1 authentication-type eap
  wlan 1 mobility enable
  wlan 1 radius server primary 127.0.0.1
@@ -184,10 +184,12 @@
  rad-user adam password 0 mypassword
  rad-user eve password 0 mypassword123
  rad-user sumi password 0 mypassword
+ rad-user test password 0 mypassword123
  rad-user vasavi password 0 mypassword123
  group kumar2
   rad-user sumi
-  policy wlan 2
+  policy vlan 44
+  policy wlan 10
  !
  group kumar3
  !
```

4.1.13 dir

▶ *Priv Exec Command*

Use this command to view the list of files on a filesystem.

Syntax

```
dir ({/all|/recursive}|) (DIR|all-filesystems|)
```

Parameters

/all	Lists all files.
/recursive	Lists files recursively.
DIR	Lists files in named file path.
all-filesystems	Lists files on all filesystems.

Example

```
RFS7000#dir
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006   cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006   cli_commands_180B.txt

RFS7000#
```

4.1.14 disable

▸ *Priv Exec Command*

Use this command to exit the Exec mode.

Syntax

```
disable
```

Parameters

None.

Example

```
RFS7000#disable
RFS7000>
```

4.1.15 edit

▶ *Priv Exec Command*

Use this command to edit a text file.

Syntax

```
edit FILE
```

Parameters

FILE	Name of the file to be edited.

Example

```
RFS7000#edit startup-config
  GNU nano 1.2.4                                      File: startup-config

!
! configuration of RFS7000 version 1.0.0.0-264B!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
!
!
!
spanning-tree mst config
 name My Name
!
crypto pki trustpoint kumar1
 subject-name "ss" ss "ss" "ss" "ss" "ss"
crypto pki trustpoint kumar2
 subject-name "ss" ss "ss" "ss" "ss" "ss"
crypto pki trustpoint thippeswamy
 subject-name "TestPool" US "OH" "PB" "MOTOROLA" "WID"
 fqdn "RetailKing.com"
 email abcTestmailid@motorola.com
 rsakey were
 company-name "RetailKing"
 password 2 1QMdio/rj0xoNM5zCnhFxlwvXMOIkDNwolSFg0N9hgBA
!
country-code us
logging console 7
snmp-server sysname RFS7000
snmp-server manager v2
snmp-server manager v3
snmp-server user snmptrap v3 encrypted auth md5
0xe111883194e13ec8f37fc14e968f9527
snmp-server user snmpmanager v3 encrypted auth md5
0xe111883194e13ec8f37fc14e968f9527
snmp-server user snmpoperator v3 encrypted auth md5
0x9a6fac33ed1241d85692b2086030eb17
ip http server
ip http secure-trustpoint default-trustpoint
ip http secure-server
.................................................................................
..........................
RFS7000#
```

4.1.16 enable

▶ *Priv Exec Command*

Use this command to turn on the privileged mode command.

Syntax

```
enable
```

Parameters

None.

Example

```
RFS7000#enable
RFS7000#
```

4.1.17 erase

▶ *Priv Exec Command*

Use this command to erase a target filesystem.

Syntax

```
erase [cf:|flash:|nvram:|startup-config:]
```

Parameters

cf	Erases contents of compact flash.
flash	Erases contents of flash.
nvram	Erases contents of nvram.
startup-config	Resets the switch configuration to factory default settings.

Example

```
RFS7000#erase cf
RFS7000#erase flash
RFS7000#erase nvram
RFS7000#erase startup-config
RFS7000#
```

4.1.18 kill

Priv Exec Command

Use this command to kill (terminate) a specified session.

Syntax

```
kill session <1-16>
```

Parameters

session	Active session. There are 16 active sessions which can be terminated.

Example

```
RFS7000#show sessions
SESSION   USER       LOCATION          IDLE         START TIME
* 1       cli       Console           00:00m      Apr 16 20:58:58 2007
  2       root      xxx.xxx.xxx.x9    00:01m      Apr 16 21:00:06 2007
RFS7000#

RFS7000#kill session 1
Please press Enter to activate this console.

RFS7000 login: cli
User Access Verification
Username: admin
Password:
Welcome to CLI

RFS7000>enable
RFS7000#
```

4.1.19 logout

▶ *Priv Exec Command*

Use this command to exit from the EXEC mode.

Syntax

```
logout
```

Parameters

None.

Example

```
RFS7000#logout
Please press Enter to activate this console.
```

4.1.20 mkdir

▸ *Priv Exec Command*

Use this command to create a new directory in the filesystem.

Syntax

```
mkdir DIR
```

Parameters

DIR	Directory name.

Example

```
RFS7000#mkdir TestDIR
RFS7000#
```

4.1.21 more

- *Priv Exec Command*

Use this command to view the contents of a file.

Syntax

```
more FILE
```

Parameters

FILE	Displays the content of the file.

Example

```
RFS7000#more flash:/log/messages.log
Sep 08 12:27:30 2006: %PM-5-PROCSTOP: Process

"radiusd" has been stopped
Sep 08 12:27:31 2006: %LICMGR-6-NEWLICENSE:

Licensed AP count changed to 48
Sep 08 12:27:31 2006: %CC-5-COUNTRYCODE:

config: setting country code to [in:
India]
Sep 08 12:27:31 2006: %DAEMON-6-INFO: radiusd

[460]: Ready to process requests.
Sep 08 12:27:35 2006: %DAEMON-6-INFO: init:

Starting pid 328, console
/dev/ttyS0
Sep 08 12:27:37 2006: %AUTH-6-INFO: login[328]:

root login  on `ttyS0' from
`Console'
Sep 08 12:27:47 2006: %IMI-5-USERAUTHSUCCESS:

User 'admin' logged in with role
of ' superuser' from auth source 'local'
Sep 08 12:28:01 2006: %NSM-6-DHCPDEFRT: Default

route with gateway
157.235.208.246 learnt via DHCP
Sep 08 12:28:01 2006: %NSM-6-DHCPIP: Interface
vlan1 acquired IP address
157.235.208.93/24 via DHCP
Sep 08 12:29:07 2006: %CC-5-RADIOADOPTED: 11bg

radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:07 2006: %CC-5-RADIOADOPTED: 11a

radio on AP 00-A0-F8-BF-8A-A2
adopted
Sep 08 12:29:12 2006: %MOB-6-MUADD: Station 00

-0F-3D-E9-A6-54: Added to
Mobility Database
Sep 08 12:29:12 2006: %CC-6-STATIONASSOC:

Station 00-0F-3D-E9-A6-54 associated
to radio 3 wlan 1
```

4.1.22 page

▶ *Priv Exec Command*

Use this command to toggle switch paging. Enabling this command displays the command output page by page, instead of running the entire output at once.

Syntax

```
page
```

Parameters

None.

Example

```
RFS7000>page ?
  <cr>

RFS7000>page

RFS7000>enable
RFS7000#show running-config
!
! configuration of RFS7000 version 1.0.0.0-280D!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
!
!
access-list 110 permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
access-list 110 permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
access-list 110 permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
!
spanning-tree mst config
 name My Na.....................................................................
.................................................................................
.................................................................................
........................
```

4.1.23 ping

▶ *Priv Exec Command*

Use this command to send ICMP echo messages.

Syntax

```
ping [IP address|hostname]
```

Parameters

[IP address|hostname]	Ping destination address or hostname.

Example

```
RFS7000#ping 111.222.222.39
PING 1111.222.222.39 (111.222.222.39): 100 data bytes
128 bytes from 111.222.222.39: icmp_seq=0 ttl=64 time=2.3 ms
128 bytes from 111.222.222.39: icmp_seq=1 ttl=64 time=0.2 ms
128 bytes from 111.222.222.39: icmp_seq=2 ttl=64 time=0.3 ms
128 bytes from 111.222.222.39: icmp_seq=3 ttl=64 time=0.2 ms
128 bytes from 111.222.222.39: icmp_seq=4 ttl=64 time=0.1 ms

--- 157.235.208.39 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.1/0.6/2.3 ms
RFS7000#
```

4.1.24 pwd

▶ *Priv Exec Command*

Use this command to view the contents of the current directory.

Syntax

pwd

Parameters

None.

Example

```
RFS7000#pwd
flash:/
RFS7000#
```

4.1.25 quit

▶ *Priv Exec Command*

Use this command to exit the current mode and move down to the previous mode.

Syntax

```
quit
```

Parameters

None.

Example

```
RFS7000#quit

RFS7000 release 1.0.0.0-264B
Login as 'cli' to access CLI.
RFS7000 login:
```

4.1.26 reload

▶ *Priv Exec Command*

Use this command to halt the switch and perform a warm reboot.

Syntax

```
reload
```

Parameters

None.

Example

```
RFS7000#reload
Wireless switch will be rebooted, do you want to continue? (y/n): y
The system is going down NOW !!

% Connection is closed by administrator!
WIOS_SECURITYMGR[1037]: FTPALG: Shutting down.
Please stand by while rebooting the system.

BootOS (c) 2004-2007 Symbol Technologies. All rights reserved.
version 1.0.0.0-280D
booting from NAND image1

Press Ctrl-D to enable debug messages during boot
Note: qchip watchdog is disabled
 0| ddr2.c:540 configure_ddr2 Clamping DIMM 0 speed at 533MHz
Invalid partition table magic number
Loading runtime image 1:
  .........................................................
Starting pmlite
Mar 15 16:57:58 2008: %LICMGR-3-LICMODIFIED: License appears to have been
mistyped
Running Primary software, version 1.0.0.0-280D
Alternate software Secondary, version 1.0.0.0-270D
Software fallback feature is enabled

Please press Enter to activate this console.


RFS7000 login: RFS7000 login: RFS7000 login:
```

4.1.27 rename

Priv Exec Command

Use this command to rename a file in the existing filesystem.

Syntax

```
rename FILE FILE
```

Parameters

FILE	FIle to rename.

Example

```
RFS7000#rename flash:/TestDIR/ NewTestDir
RFS7000#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006   cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006   cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2006   cli_commands.save
  drwx   1024      Sat Sep  2 00:31:24 2006   NewTestDir

RFS7000#
```

4.1.28 rmdir

▶ *Priv Exec Command*

Use this command to delete an existing file.

Syntax

```
rmdir DIR
```

Parameters

DIR	Name of the directory to delete.

Example

```
RFS7000#rmdir flash:/NewTestDir/
RFS7000#DIR
Directory of flash:/

  drwx   1024      Wed Jul 19 19:14:05 2006   hotspot
  drwx   120       Wed Aug 30 15:32:44 2006   log
  drwx   1024      Thu Aug 31 23:50:09 2006   crashinfo
  -rw-   14271     Tue Jul 25 15:16:41 2006   Radius-config
  -rw-   14271     Wed Jul 26 15:42:08 2006   flash:
  drwx   1024      Wed Aug  9 17:35:08 2006   radius
  -rw-   3426      Wed Jul 26 16:08:02 2006   running-config-new
  -rw-   13163     Wed Jul 26 16:08:42 2006   radius-config
  -rw-   80898     Thu Aug 17 14:59:39 2006   cli_commands.txt
  -rw-   65015     Fri Aug 11 19:57:37 2006   cli_commands.txtli_commands.txt
  -rw-   65154     Thu Aug 17 15:11:23 2006   cli_commands_180B.txt
  -rw-   32        Sat Sep  2 00:15:38 2006   cli_commands.save
```

4.1.29 show

▶ *Priv Exec Command*

Use this command to show currently running system information.

Syntax

```
show <display parameter>
```

Parameters

access-list	Displays Internet Protocol (IP) details of the access list.
aclstats	Displays ACL statistics information.
alarm-log	Displays alarms currently in the system.
autoinstall	Displays autoinstall configuration details.
banner	Displays the “Message of the Day” login banner.
boot	Displays the boot configuration.
clock	Displays the system clock.
commands	Displays the command lists.
crypto	Displays encryption related commands.
debugging	Displays debugging information outputs.
dhcp	Displays the DHCP Server configuration.
environment	Displays environmental information.
file	Displays filesystem information.
ftp	Displays the FTP server configuration.
history	Displays the session command history.
interfaces	Displays interface status.
ip	Displays Internet Protocol (IP).
ldap	Displays LDAP server data.
licenses	Displays installed license details.
logging	Displays the logging configuration and buffer.
mac	Displays MAC access-list assignment details.
mac-address-table	Displays a MAC address table.
management	Displays L3 managment Interface name details.
mobility	Displays mobility parameters.
ntp	Displays network time protocol.
password-encryption	Displays password encryption.

privilege	Displays the current privilege level.
radius	Displays RADIUS configuration commands.
redundancy-group	Displays redundancy group parameters.
redundancy-history	Displays the state transition history of the switch.
redundancy-members	Displays redundancy group members in detail.
running-config	Displays the current operating configuration.
securitymgr	Displays securitymgr parameters.
sessions	Displays current active open connections.
snmp	Displays SNMP engine parameters.
snmp-server	Displays SNMP engine parameters.
spanning-tree	Displays spanning tree information.
startup-config	Displays the contents of startup configuration.
static-channel-group	Displays static channel group membership.
terminal	Displays terminal configuration parameters.
timezone	Displays timezone.
upgrade-status	Displays the last image upgrade status.
users	Displays active user information.
version	Displays software and hardware version details.
wireless	Displays wireless configuration commands.
wlan-acl	Displays WLAN based ACL details.

Usage Guidelines

Refer to *show on page 2-25* for additional information.

Example

```
RFS7000#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                Encryption related commands
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   MAC access-list assignment
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         spanning-tree Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000#show
```

4.1.30 telnet

▶ *Priv Exec Command*

Use this command to open a telnet session.

Syntax

```
telnet [IP address|hostname]
```

Parameters

[IP address| host name]	IP address or hostname of a remote system.

Example

```
RFS7000#telnet 157.111.222.33

Entering character mode
Escape character is '^]'.

Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-6bigmem on an i686
login: cli
Password:
```

4.1.31 traceroute

▶ *Priv Exec Command*

Use this command to trace the route to a destination.

Syntax

```
traceroute (WORD | ip WORD)
```

Parameters

WORD	Traces the route to a destination address or hostname .
ip	IP trace.

Example

```
RFS7000#traceroute 157.222.333.33
traceroute to 157.235.208.39 (157.235.208.39), 30 hops max, 38 byte packets
 1  157.235.208.39 (157.235.208.39)  0.466 ms  0.363 ms  0.226 ms
RFS7000#
```

4.1.32 upgrade

▶ *Priv Exec Command*

Use this command to upgrade the switch software image.

Syntax

```
upgrade URL (background|)
```

Parameters

URL	Defines location of firmware image.

Example

```
RFS7000#upgrade tftp://xxx.xxx.xxx.xxx:/img
var2 is 10 percent full
/tmp is 2 percent full
Free Memory 161896 kB
FWU invoked via Linux shell
Running from partition /dev/hda5, partition to

update is /dev/hda6
Reading image file header
Removing other partition
Sep 08 15:57:18 2006: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
Making file system
Extracting files (this can take some time).Sep

08 15:57:23 2006: %KERN-6-INFO:
kjournald starting.  Commit interval 5 seconds.
Sep 08 15:57:23 2006: %KERN-6-INFO: EXT3 FS on

hda6, internal journal.
Sep 08 15:57:23 2006: %KERN-6-INFO: EXT3-fs:

mounted filesystem with ordered
data mode..
.........................
Sep 08 15:58:17 2006: %DIAG-4-CPULOAD: One

minute average load limit exceeded,
value is 100.00% limit is 99.90% (top process
kernel/ISR 100.00%)
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process


"logd" is not responding
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Sep 08 15:58:44 2006: %PM-4-PROCNORESP: Process

"logd" is not responding
Version of firmware update file is 1.0.0.0-264B
Sep 08 15:58:44 2006: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
Creating LILO files
Running LILO
```

```
Successful
Sep 08 15:58:46 2006: %FWU-6-FWUDONE: Firmware

update successful, new version
is 1.0.0.0-264B
RFS7000#
```

4.1.33 upgrade-abort

▸ *Priv Exec Command*

Use this command to abort an ongoing upgrade process.

Syntax

```
upgrade-abort
```

Parameters

None.

Example

```
RFS7000#upgrade-abort
% Error: No upgrade in progress

RFS7000#upgrade tftp://xxx.xxx.xxx.xxx:/img

background
RFS7000#Sep 08 16:01:38 2006: %KERN-4-WARNING:

EXT3-fs warning: maximal mount
count reached, running e2fsck is recommended.
Sep 08 16:01:38 2006: %KERN-6-INFO: EXT3 FS on

hda1, internal journal.
%KERN-6-INFO: kjournald starting.  Commit

interval 5 seconds.
Sep 08 16:01:43 2006: %KERN-6-INFO: EXT3 FS on

hda6, internal journal.
Sep 08 16:01:43 2006: %KERN-6-INFO: EXT3-fs:

mounted filesystem with ordered
data mode..
RFS7000#upgrade-abort
RFS7000#
RFS7000#show upgrade-status
Last Image Upgrade Status : Extracting files

(this can take some time).Aborted
Last Image Upgrade Time   : Fri Sep  8 16:01:54 2006
```

4.1.34 write

- *Priv Exec Command*

Use this command to write the running configuration to memory or terminal

Syntax

```
write [memory | terminal]
```

Parameters

memory	Writes to NV memory.
terminal	Writes to terminal.

Example

```
RFS7000#write terminal
!
! configuration of RFS7000 version 1.0.0.0-264B!
version 1.0
!
service prompt crash-info
!
username admin password 1 8e67bb26b358e2ed20fe552ed6fb832f397a507d
username admin privilege  superuser
username operator password 1 fe96dd39756ac41b74283a9292652d366d73931f
username manager password 1 45b27d6483fc630981ad5096ff26a7956ce0c038
username manager privilege  superuser
!
!no country-code
logging console 7
no logging on
fallback enable
ftp password 1 810a25d76c31e495cc070bdf42e076f7c9b0a1cd
ip http server
ip http secure-trustpoint local
ip http secure-server
ip ssh
ip telnet
snmp-server manager v2
snmp-server manager v3
crypto isakmp identity address
crypto isakmp keepalive 10
!.......................................
```

5

Global Configuration Commands

The term **global** is used to indicate characteristics or features effecting the system as a whole. Use the Global configuration mode to configure the system globally, or enter specific configuration modes to configure specific elements (such as interfaces or protocols). Use the *configure terminal* command, under PRIV EXEC, to enter global configuration mode.

The example below describes entering the global configuration mode from the privileged EXEC mode:

```
RFS7000# configure terminal
RFS7000(config)#
```

NOTE The system prompt changes to indicate you are in global configuration mode. The prompt for global configuration mode consists of the host-name of the device followed by (config) and the pound sign (#).

Commands entered in the global configuration mode update the running configuration file as soon as they are entered. However, these changes are not saved in the startup configuration file until a *copy running-config startup-config* EXEC mode command is issued.

5.1 Global Configuration Commands

Table 5.1 summarizes the Global Config commands.

Table 5.1 Global Configuration Command Summary

Command	Description	Ref.
aaa	Authentication, Authorization and Accounting.	page 5-4
access-list	Adds an access list entry.	page 5-5
autoinstall	Autoinstalls a configuration command.	page 5-11
banner	Defines a login banner.	page 5-12
boot	Reboots the switch.	page 5-13
bridge	Bridgse group commands.	page 5-14
clrscr	Clears the display screen.	page 2-3
country-code	Configures the country of operation. This erases all existing radio configuration.	page 5-15
crypto	Encryption related commands.	page 5-17
debug	Debugging functions.	page 5-19
do	Runs commands from EXEC mode.	page 5-20
end	Ends the current mode and change to the EXEC mode.	page 5-21
exit	Ends the current mode and moves down to the previous mode.	page 2-10
format	Formats file system.	page 5-22
ftp	Configures FTP server.	page 5-23
help	Description of the interactive help system.	page 2-11
hostname	Sets the system's network name.	page 5-24
interface	Select an interface to configure.	page 5-25
ip	Internet Protocol (IP).	page 5-26
license	License management command.	page 5-30
line	Configures a terminal line.	page 5-31
logging	Modifies message logging facilities.	page 5-32
mac	Configures MAC ACLs.	page 5-34
management	Sets properties of the management interface.	page 5-35
no	Negates a command or set its defaults .	page 2-12
ntp	Configures NTP.	page 5-36

Command	Description	Ref.
prompt	Sets the system prompt.	page 5-39
radius-server	Enters radius-server mode.	page 5-40
redundancy	Configures redundancy group parameters.	page 5-41
service	Service commands.	page 5-43
show	Shows running system information. Refer to *Global Config* show commands.	page 2-25
snmp-server	Modifies SNMP engine parameters.	page 5-48
spanning-tree	Spanning tree commands.	page 5-57
timezone	Configures the timezone.	page 5-60
username	Establishes user name authentication.	page 5-61
wireless	Configures wireless parameters.	page 5-62
wlan-acl	Applies an ACL on the WLAN port.	page 5-63

5.1.1 aaa

▶ *Global Configuration Commands*

Use this command to configure the current *Authentication,Authorization and Accounting* (aaa) login settings.

Syntax

```
aaa authentication login default
[local{none|radius(none)}|none| radius{local(none)|none}]
```

Parameters

authentication	Authentication configuration parameters.
login	Sets an authentication list for logins.
default	The default authentication list.
local	Uses local user database.
none	No authentication.
radius	Uses external RADIUS server.

Usage Guidelines

Use AAA login to determine whether management user authentication must be performed against a loacl user database or a external RADIUS server.

Example

```
RFS7000(config)#username motorolaadmin password motorola

RFS7000(config)#username motorolaadmin privilege  superuser

RFS7000(config)#aaa authentication login default local
RFS7000(config)#
```

5.1.2 access-list

Global Configuration Commands

Use this command to add an access list entry. Use the access list command under global configuration to configure the access list mechanism for filtering frames by protocol type or vendor code.

Syntax

```
access-list
```

For Standard IP ACL's:

```
access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-7> | tos <0-
255>))(A.B.C.D/M | host A.B.C.D | any)(log) (rule-precedence <1-5000>)
```

For Extended IP ACL's:

```
access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-7> | tos <0-
255>}} {ip} {source/source-mask | host source | any } {destination/destination-
mask  | host destination | any } [log] [rule-precedence access-list-entry
precedence]

access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-7> | tos <0-
255>}} {icmp} {source/source-mask | host source | any} {destination/ destination-
mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-
precedence access-list-entry precedence]

access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-7> | tos <0-
255>}} {tcp|udp} {source/source-mask | host source | any} [operator source-port]
{destination/destination-mask | host destination | any} [operator destination-
port] [log] [rule-precedence access-list-entry precedence]
```

NOTE Using `access-list [<100-199>|<2000-2699>]` leads you to the **`(config-ext-nacl)`** instance. For additional information, see *Extended ACL Instance on page 9-1*.

Using `access-list [<1-99>|<1300-1999>]` leads you to the **`(config-std-nacl)`** instance. For additional information, see *Standard ACL Instance on page 10-1*.

To create a named ACL, use `ip access-lsit` (Standard/Extended). For more details check *ip on page 5-26*.

Parameters

access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-7> | tos <0-255>)) (A.B.C.D/M | host A.B.C.D | any)(log) (rule-precedence <1-5000>)	Add a standard access list entry. • (<1-99>|<1300-1999>) – Access numbers from 1 to 99 or 1300 to 1999. • (deny|permit|mark) – Action types on an ACL. The action type `mark` is functional only over a Port ACL. • 8021p <0-7> – Used only with the action type `mark` to specify 8021p priority values.e • tos <0-255> – Used only with thction type `mark` to specify *type of service* (tos) values. • (A.B.C.D/M | host A.B.C.D | any) – Source is the source address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • The keyword **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0. • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32. • log – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. • (rule-precedence <1-5000>) – Integer value between 1-5000. This value sets the rule precedence in the ACL.

access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-7> | tos <0-255>}} {**ip**} {source/source-mask | host source | any } {destination/destination-mask | host destination | any } [log] [rule-precedence access-list-entry precedence]	Add an Extended IP access list entry using **IP** keyword. • <100-199>|<2000-2699> – For IP type of extended ACL, the ACL number must be between 100-199. • {deny | permit | mark {dot1p <0-7> | tos <0-255>}} – Action types on an ACL. The action type `mark` is functional only over a Port ACL. • 8021p <0-7> – Used only with the action type `mark` to specify 8021p priority values. • tos <0-255> – Used only with action type `mark` to specify *type Of service* (tos) values. • {**ip**} – Specify ip (to match any protocol) • {source/source-mask | host source | any } – Source is the source address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • The keyword **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0. • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32. • {destination/destination-mask | host destination | any } – The destination host IP address or destination network address. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-7> | tos <0-255>}} {**icmp**} {source/source-mask | host source | any} {destination/ destination-mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-precedence access-list-entry precedence]	Add an Extended IP access list entry using **icmp** keyword. • (<100-199>|<2000-2699>) – For ICMP extended ACLs, the ACL number must be between 2000-2699. • {deny | permit | mark {dot1p <0-7> | tos <0-255>}} – Action types on an ACL. The action type `mark` is functional only over a Port ACL. • {**icmp**} – Specify icmp as protocol. • {source/source-mask | host source | any} – Source is the source address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • The keyword **any** is an abbreviation for source an IP of 0.0.0.0 and source-mask bits equal to 0. • The keyword **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32. • {destination/ destination-mask | host destination | any} – The destination host IP address or destination network address. • [icmp-type |icmp-type icmp-code] – **ICMP type** value from 0 - 255. Valid only for protocol type icmp. **ICMP code** value from 0 - 255. Valid only for a protocol type of icmp. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

access-list (<100-199>|<2000-2699>) {deny | permit | mark {dot1p <0-7> | tos <0-255>}} {**tcp|udp**} {source/source-mask | host source | any} [operator source-port] {destination/destination-mask | host destination | any} [operator destination-port] [log] [rule-precedence access-list-entry precedence]	Add an Extended IP access list entry using **tcp or udp** keyword. • (<100-199>|<2000-2699>) – For tcp or udp type of extended ACL, the ACL number must be between 2000-2699. • {deny | permit | mark {dot1p <0-7> | tos <0-255>}} – Action types on an ACL. The action type `mark` is functional only over a Port ACL. • {**tcp|udp**} – Specifies tcp or udp as the protocol. • {source/source-mask | host source | any} – Source is the source address of the network or host in dotted decimal. Source-mask is the network mask. For e.g. 10.1.1.10/24 indicates that the first 24 bits of the source IP are used for matching. • **any** is an abbreviation for a source IP of 0.0.0.0 and source-mask bits equal to 0. • **host** is an abbreviation for an exact source (A.B.C.D) and source-mask bits equal to 32. • [operator source-port] – Valid only for tcp or udp protocols. Valid values are **eq** and **range**. • range – Specify the protocol range (starting and ending protocol numbers). • port – Valid Port number. • {destination/destination-mask | host destination | any} – The destination host IP address or destination network address. • [operator destination-port] – Specify the destination port. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACL's. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Use an access list command under global configuration to create an access list. RFS7000 supports port, router and WLAN ACL's.

- When the access list is applied on an Ethernet port, it becomes a port ACL.
- When the access list is applied on a VLAN interface, it becomes a router ACL.
- When the access list is applied on a WLAN index, it becomes a WLAN ACL.

A MAC access list, to allow arp, is mandatory for both port and WLAN ACL's. For more information on how to configure a MAC access list, see *permit on page 11-12*

Example

The example below creates a standard *access list* (ACL) to permit any traffic coming to the interface.

```
RFS7000(config)#access-list 1 permit any
RFS7000(config)#
```

The example below creates a extended IP access list to permit IP traffic between two networks.

```
RFS7000(config)#access-list 101 permit ip 192.168.1.0/24 192.168.2.0/24
RFS7000(config)#
```

The example below creates a extended access list to permit tcp traffic, between two networks, with destination port range between 20 and 23.

```
RFS7000(config)#access-list 101 permit tcp 192.168.1.0/24 192.168.2.0/24 range 20
23
RFS7000(config)#
```

The example below denies icmp traffic from any source to any destination.

```
RFS7000(config)#access-list 115 deny icmp any any
RFS7000(config)#access-list 115 permit ip any any
RFS7000(config)#
```

5.1.3 autoinstall

▸ *Global Configuration Commands*

Use this command to autoinstall the switch image.

Syntax

```
autoinstall [clear-config-history|cluster-config|config|image|start]
autoinstall (cluster-config|config|image) (URL[tftp|ftp|http|cf])

autoinstall image version <number>
```

Parameters

clear-config-history	Autoinstalls a clear configuration history, resulting in a reversion.
cluster-config	Autoinstalls a cluster-config setup.
config	Autoinstalls a config setup.
image <*version number*>	Autoinstalls the image setup. • Version number – the version number cannot be the same as the currently installed version number. Attempting to install the same version results in an unsuccesfull download.
start	Starts the autoinstall sequence.

Example

```
RFS7000(config)#autoinstall clear-config-history
RFS7000(config)#
```

5.1.4 banner

▶ *Global Configuration Commands*

Use this command to define a login banner for the switch.

Syntax

```
banner(motd(LINE|default))
```

Parameters

motd	Sets the “message of the day” banner.
LINE	Custom MOTD string.
default	Default MOTD string.

Example

```
RFS7000(config)#banner motd Welcome to my RFS7000 CLI
RFS7000(config)

RFS7000 release 3.0.0.0-200B
Login as 'cli' to access CLI.
RFS7000 login: cli
Welcome to my RFS7000 CLI
Welcome to my RFS7000 CLI
RFS7000>

RFS7000(config)#banner motd default
RFS7000(config)#

RFS7000 release 3.0.0.0-200B
Login as 'cli' to access CLI.
RFS7000 login: cli
Welcome to CLI
Welcome to CLI

RFS7000>
```

5.1.5 boot

▶ *Global Configuration Commands*

This command reboots the switch with an image present in the mentioned partition (either the primary or secondary partition).

Syntax

```
boot(system [primary|secondary])
```

Parameters

system	Specifies the boot image used after reboot.
primary	Specifies the primary image.
secondary	Specifies the secondary image.

Example

```
RFS7000(config)#boot system primary
Wireless switch will be rebooted, do you want to continue? (y/n):y
Do you want to save the configuration? (y/n):y

The system is going down NOW !!

% Connection is closed by administrator!
Please stand by while rebooting the system.
```

5.1.6 bridge

▶ Global Configuration Commands

Configures bridge specific details.

Syntax

```
bridge [<1-32>|multiple-spanning-tree]

bridge <1-32> [address|ageing-time]

bridge <1-32> (address)MAC [discard|forward](NAME|fe|ge|sa|tunnel|vlan)
bridge <1-32> (address)MAC [discard|forward] fe (vlan <2-4094>)
bridge <1-32> (address)MAC [discard|forward] ge <1-4> (vlan <2-4094>)
bridge <1-32> (address)MAC [discard|forward] sa <1-4> (vlan <2-4094>)
bridge <1-32> (address)MAC [discard|forward] tunnel <1-32> (vlan <2-4094>)
bridge <1-32> (address)MAC [discard|forward] vlan <1-4094> (vlan <2-4094>)

bridge <1-32> (ageing-time)<10-1000000>

bridge multiple-spanning-tree (enable)
```

Parameters

<1-32> [address|ageing-time]	The bridge groups available for bridging. • address – Address of the bridge group selected for bridging. • ageing-time – Time a learned MAC address persists after last update.
(address) MAC [discard|forward] (NAME|fe|ge|sa|tunnel| vlan)	MAC address of the interface selected for bridging. The MAC address must be in `HHHH.HHHH.HHHH` format. • discard – Discard the MAC address. • forward – Forward the MAC address. • NAME – Interface name. • fe (vlan <2-4094>) – FastEthernet interface. • ge <1-4> (vlan <2-4094>) – GigabitEthernet interface index. • sa <1-4> (vlan <2-4094>) – StaticAggregate interface index. • tunnel <1-32> (vlan <2-4094>) – Tunnel interface index. • vlan <1-4094> (vlan <2-4094>) – VLAN interface index.
<1-32> (ageing-time) <10-1000000>	Time a learned MAC address persists after last update. • (ageing-time) <10-1000000> – Ageing time in seconds.
multiple-spanning-tree (enable)	Enables *Multiple Spanning Tree Protocol* (MSTP) commands.

Usage Guidelines

Use `bridge multiple-spanning-tree` command to enable or disable MSTP globally. Use `no` command with bridge-forward parameter to disable MSTP and change all ports to forwarding state.

Example

```
RFS7000(config)#bridge multiple-spanning-tree enable
RFS7000(config)
```

5.1.7 country-code

Global Configuration Commands

Use this command to configure the country of operation.

Syntax

```
country-code
```

Parameters

None.

Usage Guidelines

This command erases all existing radio configuration.

Example

```
RFS7000(config)#country-code ?
  ae  United Arab Emirates
  ar  Argentina
  at  Austria
  au  Australia
  ba  Bosnia Herzegovina
  be  Belgium
  bg  Bulgaria
  bh  Bahrain
  bm  Bermuda
  br  Brazil
  bs  Bahamas
  by  Belarus
  ca  Canada
  ch  Switzerland
  cl  Chile
  cn  China
  co  Colombia
  cr  Costa Rica
  cy  Cyprus
  cz  Czech Republic
  de  Germany
  dk  Denmark
  do  Dominican Republic
  ec  Ecuador
  ee  Estonia
  eg  Egypt
  es  Spain
  fi  Finland
  fr  France
  gb  United Kingdom
  gr  Greece
  gt  Guatemala
  gu  Guam
  hk  Hong Kong
  hn  Honduras
  hr  Croatia
  ht  Haiti
  hu  Hungary
  id  Indonesia
  ie  Ireland
  il  Israel
  in  India
  is  Iceland
  it  Italy
  jo  Jordan
  jp  Japan
  kr  South Korea
```

```
 kw  Kuwait
 kz  Kazakhstan
 li  Liechtenstein
 lk  Sri Lanka
 lt  Lithuania
 lu  Luxembourg
 lv  Latvia
 ma  Morocco
 mt  Malta
 mx  Mexico
 my  Malaysia
 nl  Netherlands
 no  Norway
 nz  New Zealand
 om  Oman
 pe  Peru
 ph  Philippines
 pk  Pakistan
 pl  Poland
 pt  Portugal
 qa  Qatar
 ro  Romania
 ru  Russia
 sa  Saudi Arabia
 se  Sweden
 sg  Singapore
 si  Slovenia
 sk  Slovak Republic
 th  Thailand
 tr  Turkey
 tw  Taiwan
 ua  Ukraine
 us  United States
 uy  Uruguay
 ve  Venezuela
 vn  Vietnam
 za  South Africa
RFS7000(config)#country-code
```

5.1.8 crypto

▶ *Global Configuration Commands*

Use this command to configure encryption related commands.

☑ **NOTE** `crypto pki trustpoint` mode leads to `(config-trustpoint)` instance. For more information, see *crypto-trustpoint Instance on page 6-1*.

Syntax

```
crypto(key|pki)

crypto key(export|generate|import|zeroize)
crypto key export rsa<name> URL[tftp|ftp]
crypto key generate rsa<name> <1024-2048>
crypto key import rsa<name> URL[tftp|ftp]
crypto key zeroize rsa<name>

crypto pki(authenticate|enroll|export|import|trustpoint)
crypto pki authenticate <name> (terminal|tftp|ftp)
crypto pki enroll<name> (request|self-signed)
crypto pki export <name> (request|trustpoint)(tftp|ftp)
```

Parameters

key	Authentication key management.
export	Exports a keypair related configuration.
generate	Generates a keypair.
import	Imports keypair related configuration.
zeroize	Deletes a keypair.
rsa<identifier>	RSA keypair identifier associated with keypair.
URL	URL for sending the key to. It can be one of the following: • `tftp://<IP>/path/file` (or) • ftp://<user>:<passwd>@<IP>/path/file
pki	Configures certificate parameters. The public key infrastructure is a protocol that creates encrypted public keys using digital certificates from certificate authorities. PKI ensures each online party is who they claim to be.
authenticate	Authenticate and import CA certificate.
enroll	Enroll.
export	Export.
import	Import.
trustpoint	Defines a CA trustpoint.
request	Certificate request mode of enrollment.

self-signed	Selfsigned mode of enrollment.
trustpoint	Trustpoint configuration.
terminal	Copies and pastes enrollment mode.

Usage Guidelines

Use crypto pki with diffrent parameters to configure trustpoint and its parameters. Use crypto key to configure RSA key pairs.

Example

```
RFS7000(config)#crypto pki ?
  authenticate  Authenticate and import CA Certificate
  enroll        Enroll
  export        Export
  import        Import
  trustpoint    Define a CA trustpoint

RFS7000(config)#crypto pki trustpoint ?
  WORD  Trustpoint Name

RFS7000(config)#crypto pki trustpoint Test
RFS7000(config-trustpoint)#?
Trustpoint Config commands:
  clrscr        Clears the display screen
  company-name  Company Name(Applicable only for request)
  email         email
  end           End current mode and change to EXEC mode
  exit          End current mode and down to previous mode
  fqdn          Domain Name Configuration
  help          Description of the interactive help system
  ip-address    Internet Protocol (IP)
  no            Negate a command or set its defaults
  password      Challenge Password(Applicable only for request)
  rsakeypair    Rsa Keypair to associate with the trustpoint
  service       Service Commands
  show          Show running system information
  subject-name  Subject Name is a collection of required parameters to
                configure a trustpoint.

RFS7000(config-trustpoint)#
```

5.1.9 debug

▶ *Global Configuration Commands*

Use this command to turn on and off mstp debugging messages.

Syntax

```
debug (mstp) [all|cli|packet(rx |tx)|protocol (detail)|timer(detail)]
```

Parameters

all	Echoes all MSTP debugging levels to the console.
cli	Echoes all MSTP debugging levels to the console.
packet	Echoes MSTP packets (received and transmitted) to the console.
protocol (detail)	Echoes protocol changes to the console. • detail – Detailed output.
timer (detail)	Echoes timer start to the console. • detail – Detailed output.

Example

```
RFS7000(config)#debug mstp all
RFS7000(config)#

RFS7000(config)#debug mstp cli
RFS7000(config)#

RFS7000(config)#debug mstp packet rx
RFS7000(config)#

RFS7000(config)#debug mstp protocol detail
RFS7000(config)#

RFS7000(config)#debug mstp timer detail
RFS7000(config)#
```

5.1.10 do

▶ *Global Configuration Commands*

Use this command to run commands from either the User Exec or Priv Exec mode.

Syntax

```
do (command of other mode)
```

Parameters

None.

Example

```
RFS7000(config)#do ping 157.235.208.69
PING 157.235.208.69 (157.235.208.69): 100 data bytes
128 bytes from 157.235.208.69: icmp_seq=0 ttl=64 time=0.1 ms
128 bytes from 157.235.208.69: icmp_seq=1 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=2 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=3 ttl=64 time=0.0 ms
128 bytes from 157.235.208.69: icmp_seq=4 ttl=64 time=0.0 ms

--- 157.235.208.69 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.1 ms
RFS7000(config)#
```

☑ **NOTE** In the example above, `ping` is a PRIV EXEC command.

5.1.11 end

▶ *Global Configuration Commands*

Use this command to end the current mode and change to the Exec mode.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config)#end

RFS7000#?
Priv Exec commands:
  acknowledge    Acknowledge alarms
  archive        Manage archive files
  autoinstall    autoinstall configuration command
  cd             Change current directory
  ............................................
  ............................................
```

5.1.12 format

▶ *Global Configuration Commands*

Use this command to format the *Compact Flash* (CF) card.

Syntax

```
format
```

Parameters

cf	Format compact flash.

Example

```
RFS7000(config)#format cf
RFS7000(config)#
```

5.1.13 ftp

▶ *Global Configuration Commands*

Use this command to configure the switch as an FTP server.

Syntax

```
ftp enable
ftp password(0|1|LINE)
ftp rootdir(DIR)
```

Parameters

enable	Enables FTP server.
password	Configures a FTP password. Set the password using one of the folllowing: • 0 — Password is specified UNENCRYPTED. • 1 — Password is encrypted with SHA1 algorithm. • LINE — Password.
rootdir	Configures the FTP root dir. Set the ROOT directory location of the FTP server using: • DIR — Sets root dir of the ftp server.

Example

```
RFS7000(config)#ftp enable
RFS7000(config)#
```

5.1.14 hostname

▶ *Global Configuration Commands*

Use this command to change the system’s network name.

Syntax

```
hostname(WORD)
```

Parameters

WORD	Use this command to provide the name for the network.

Example

```
RFS7000(config)#hostname Eldorado
Eldorado(config)#
```

5.1.15 interface

▶ *Global Configuration Commands*

Use this command configure a selected interface.

> ☑ **NOTE** The interface mode leads to the `config-if` instance. For additional information, see *interface Instance on page 7-1*.
>
> The prompt changes from `RFS7000(config) #` to `RFS7000(config-if)`

Syntax

```
interface(IFNAME|fe|ge <1-4>|sa <1-4>|tunnel <1-32>|vlan <1-4094>)
```

Parameters

IFNAME	Interface name.
ge <1-4>	GigabitEthernet interface. Select an index value between 1 - 4.
me1	FastEthernet interface.
sa <1- 4>	StaticAggregate interface. Select an index value between 1 - 4.
tunnel <1-32>	Tunnel interface. Select an index value between 1 - 32.
vlan <1-4092>	VLAN interface. Select an index value between 1 - 4092.

Example

```
RFS7000(config)#interface me1
RFS7000(config-if)#

RFS7000(config)#interface ge 3
RFS7000(config-if)#

RFS7000(config)#interface sa 2
RFS7000(config-if)#

RFS7000(config)#interface tunnel 27
RFS7000(config-if)#

RFS7000(config)#interface vlan 400
RFS7000(config-if)#
```

5.1.16 ip

▶ *Global Configuration Commands*

Use this CLI command to configure a selected Internet Protocol.

NOTE Use an `ip access-list extended` command to move to the **`(config-ext-nacl)`** instance. For additional information, see *Extended ACL Instance on page 9-1*.

Use an `ip access-list standard` command to move to the **`(config-std-nacl)`** instance. For additional information, see *Standard ACL Instance on page 10-1*.

Use an `ip dhcp pool (pool name)` command to move to the **`( config-dhcp)`** instance. For additional information, see *DHCP Instance on page 12-1*.

Syntax

```
ip(access-list|default-gateway|dhcp|domain-lookup|domain-name|http|name-
server|nat|route|routing|ssh|telnet)

ip access-list [extended{<100-199|<2000-2699>|WORD}|standard{<1-99>|<1300-
1999>|WORD}]

ip default-gateway(A.B.C.D)

ip dhcp [bootp|excluded-address|option|ping|pool|restart]
ip dhcp bootp(ignore)
ip dhcp excluded-address(A.B.C.D)
ip dhcp option(option name)
ip dhcp ping(timeout <1-10>)
ip dhcp pool(pool name)
ip dhcp restart

ip domain-lookup

ip domain-name(WORD)

ip http [secure-server|secure-trustpoint(WORD)|server(localhost)]

ip local [pool(default {low-ip-address(A.B.C.D)})]

#ip name-server(A.B.C.D)

ip nat <inside | outside> source list <access-list name> interface <interface
name> overload

ip nat <inside | outside> <source | destination> static <local-ip> [<tcp|udp> <1-
65535>] <nat-ip> <1-65535>
ip route(A.B.C.D|A.B.C.D/M)

ip routing

ip ssh(port|rsa)
ip ssh(port(<0-65536>))
ip ssh [rsa {keypair-name(WORD)}]

ip telnet [port(<0-65535>)]
```

Parameters

access-list	Use the access list parameter to enter the **`ext-nacl`** context and **`std-nacl`** context. The prompt changes to the context entered. For additional information, see *Extended ACL Instance on page 9-1* (for extended ACLs) and *Standard ACL Instance on page 10-1* (for standard ACLs).
default-gateway	Configures the default gateway.
A.B.C.D	IP gateway address.
dhcp	DHCP Server configuration.
bootp	BOOTP specific configuration.
ignore	Configures the DHCP Server to ignore BOOTP requests.
excluded-address	Prevents the DHCP Server from assigning certain addresses.
A.B.C.D	Low IP Address.
option	Defines the DHCP server option name.
ping	Specifies the ping parameters used by DHCP server.
timeout	Specifies a ping timeout between 1-10 seconds.
pool	Configures the DHCP Server address pool.
restart	Restart DHCP Server to get the DHCP config changes into effect.
domain-lookup	Enables the *Domain Name Service* (DNS).
domain-name	Sets default domain for DNS.
http	Hyper Text Transfer Protocol (HTTP).
secure-server	Secure HTTP server (HTTPS).
secure-trustpoint	Enter the name of the trustpoint to be used for secure connection.
server	HTTP server.
localhost	Used only to serve requests from localhost.
local	vpn local ip pool configuration.
pool	Address pool.
default	
low-ip-address	
A.B.C.D	Internet Protocol.
name-server	Adds a nameserver to the DNS.
A.B.C.D	IP address of Nameserver to add.
nat	*Network Address Translation* (NAT).

ip nat <inside | outside> source list <access-list name> overload interface <interface name>	• <*inside*|*outside*> – Defines the interface as private (inside) or public (external). NAT translations refer to this keyword to identify the translations applied to incoming packets on an interface. Refer to *ip on page 7-9* for details on marking an interface as private (inside) or public (external). • source list <access-list name> – Use the keyword `source` to add source address translation. Use the keyword `list` (access list) to specify the intresting traffic for NAT. This NAT's the source IP address of the traffic matching the access list. • interface <interface name> overload– Public or outgoing interface name. The source IP address of the traffic gets translated to the IP adress of the selected interface. **Note** Use this command to configure port NAT.
ip nat <inside | outside> <source | destination> static <local-ip> [<tcp|udp> <1-65535>] <nat-ip> <1-65535>	• <source|destination> – Specifies to NAT the source or destination IP address of packet. • static <local IP> – Identifies the translation as a static transaltion and identifies the IP address of the incoming packet. • <tcp|udp> <1-65535> – Selects the desired IP protocol type and port number for the incoming packet. • <nat-ip> <1-65535> – NATed IP address and port number to which the packets IP address and port number must be changed. The port number <1-65535> is valid only for destination NAT. **Note** Use this command to configure static NAT.
route	Establish static routes. • A.B.C.D – IP destination prefix. • A.B.C.D/M – IP destination prefix.
routing	Turn on IP routing.
ssh	Secured Shell (SSH) Server. • port– Listening port. The value can be between 0-65536. • rsa – RSA encryption key. • keypair-name – Configures a RSA keypair used for encryption. • WORD – RSA keypair name.
telnet	Telnet server. • port – Value of the listening port. The value can be between 0-65535.

Usage Guidelines

By using the `ip access-list` parameter you enter the following contexts:

- ext-nacl — Extended ACL. For more details see *Extended ACL Instance on page 9-1*.
- std-nacl — Standard ACL. For more details see *Standard ACL Instance on page 10-1*.
- Use *clear* command to clear the ip dhcp binding.

NOTE To delete Standard/Extended and MAC ACL use **no access-list <access-list name>** under the *Global Config* mode.

Network Address Translation (NAT) allows a single device to act as a gateway for internal LAN clients. It translates the clients internal network IP adresses into the IP address of the NAT enabled device.

RFS7000 supports port NAT and static NAT.

- Static NAT allows host on a private network and is accessible through internet using public IP's.
- Static NAT assigns a public IP to a host on a private network. It allows a host on a public network to communicate with the host on the private network, using its public IP.
- Port NAT maps multiple local addresses to a single global address and dynamic port numbers.

Use `ip nat inside` to mark VLAN interfaces as an inside interface. The keyword `inside` defines the VLAN interface as internal interface. This command is used in the `(config-if)` mode, check *ip on page 7-9* for more detials.

Example

The example below creates a named extended IP access list.

```
RFS7000(config)#ip access-list extended TestACL
RFS7000(config-ext-nacl)#
```

The example below creates a named standard IP access list.

```
RFS7000(config)#ip access-list standard TestStdACL
RFS7000(config-std-nacl)#
```

The example below creates a static NAT translation.

```
RFS7000(config)#ip nat inside destination static 1.1.1.1 2.2.2.2
RFS7000(config)#
```

The example below creates a DHCP pool.

```
RFS7000(config)#ip dhcp pool TestPool
RFS7000(config-dhcp)#
```

5.1.17 license

▶ Global Configuration Commands

Use this command to see the details of the license.

Syntax

```
license
```

Parameters

WORD	Enter the name of the feature for which you wish to add a license.

Example

```
RFS7000(config)#show licenses
Serial Number 6283529900020
  feature          license string                                 license value  usage
  AP                                                              256            4

RFS7000(config)#
```

5.1.18 line

▶ *Global Configuration Commands*

Use this command to configure the terminal line.

NOTE Using the `line vty` command moves you to the **`(config-line)`** instance.

Syntax

```
line(console|vty)
```

Parameters

console	Primary terminal line.
vty	Virtual terminal. Configure a value between 0-871.

5.1.19 logging

▶ *Global Configuration Commands*

Use this command to modify message logging facilities.

Syntax

```
logging(aggregation-time|buffered|console|facility|host|monitor|on|syslog)

logging aggregation-time(<1-20>)

logging buffered(<0-7>|alerts|critical|debugging|emergencies|errors|
informational|notifications|warnings)
```

Parameters

aggregation-time	Sets number of seconds (between 1 - 120) for aggregating repeated messages.
buffered	Sets the buffered logging level.
console	Sets the console logging level.
monitor	Sets the terminal line logging level.
syslog	Sets the syslog servers logging level.
<0-7>	Enters the logging severity level (between 0 - 7)
alerts	Immediate action needed, (severity=1).
critical	Critical conditions, (severity=2).
debugging	Debugging messages, (severity=7).
emergencies	System is unusable, (severity=0).
errors	Error conditions, (severity=3).
informational	Informational messages, (severity=6).
notifications	Normal but significant conditions, (severity=5).
warnings	Warning conditions, (severity=4).
facility	Syslog facility in which log messages are sent.
local0	Syslog facility local0.
local1	Syslog facility local1.
local2	Syslog facility local2
local3	Syslog facility local3.
local4	Syslog facility local4.
local5	Syslog facility local5.
local6	Syslog facility local6.
local7	Syslog facility local7.

host	Configures the remote host to receive log messages.
A.B.C.D	Remote host's IP address.
on	Enables the logging of system messages.

Example

```
RFS7000(config)#logging aggregation-time 20
RFS7000(config)#
```

5.1.20 mac

- *Global Configuration Commands*

Use this command to configure MAC access-lists.

Syntax

```
mac(access-list(extended(WORD)))
```

Parameters

access-list (extended <name>)	Enter a name for MAC extended ACL.

Usage Guidelines

To delete a Standard/Extended or MAC ACL, use **`no access-list <access-list name>`** under the Global Config mode.

Example

```
RFS7000(config)#mac access-list extended Test1
RFS7000(config-ext-macl)#
```

☑ **NOTE** By using the `mac access-list` parameter, the following contexts is supplied:

- ext-macl — Extended MAC ACL. For additional information, see *Extended MAC ACL Instance on page 11-1*

5.1.21 management

▶ *Global Configuration Commands*

Use this command to set management interface properties.

Syntax

```
management(secure)
```

Parameters

secure	Limits local access (Web/Telnet etc.) to the management interface.

Example

```
RFS7000(config)#management secure
RFS7000(config)#
```

5.1.22 ntp

Global Configuration Commands

Use this command to configure NTP.

Syntax

```
ntp(access-group|authenticate|authentication-key|autokey|
broadcast|broadcastdelay|master|peer|server|trusted-key)

ntp access-group(peer|query-only|serve|serve-only)
ntp access-group peer(<1-99>|<1300-1999>)
ntp access-group query-only(<1-99>|<1300-1999>)
ntp access-group serve(<1-99>|<1300-1999>)
ntp access-group serve-only(<1-99>|<1300-1999>)

ntp authenticate

ntp authentication-key <1-65534>

ntp autokey(client-only|host)

ntp broadcast(client|destination)
ntp broadcast destination(<name>(key<1-65534>|version<1-4>))

ntp broadcastdelay <1-999999>

ntp master <1-15>

ntp peer<name>
ntp peer <name>(autokey|key|prefer|version)
ntp peer <name> autokey(prefer|version<1-4>)
ntp peer <name> key(<1-65534>(prefer|version(<1-4>)))
ntp peer <name> prefer (version<1-4>)
ntp peer <name> version<1-4>

ntp server<Peer IP>
ntp server <Peer IP>(autokey|key|prefer|version)
ntp server <Peer IP> autokey(prefer|version<1-4>)
ntp server <Peer IP> key(<1-65534>(prefer|version(<1-4>)))
ntp server <Peer IP> prefer (version<1-4>)
ntp server <Peer IP> version<1-4>

ntp trusted-key <1-65534>
```

Parameters

access-group	Controls NTP access.
peer	Provides full access.
query-only	Allows only control queries.
serve	Provides server and query access.
serve-only	Provides server access only.
<1-99>	Standard IP access list.
<1300-1999>	Standard IP access list (expanded range).
authenticate	Authenticates time sources.

authentication-key *<1-65534>*	Define an authentication key for trusted time sources. Select a keynumber between 1 and 65534.
autokey	Enables NTP autokey authentication scheme.
client-only	Switch will be a client to other trusted-hosts in the autokey group.
host	Configures the switch as a trusted host.
broadcast	Configures NTP broadcast service.
client	Listens to NTP broadcasts.
destination	Configures broadcast destination address.
WORD	Destination broadcast IP address.
key	Broadcast key.
<1-65534>	Key ID.
version	NTP version.
<1-4>	NTP Version number.
broadcastdelay	Estimated round-trip delay.
<1-999999>	Round-trip delay in microseconds.
master	Acts as a NTP master clock.
<1-15>	Starting number for the NTP master clock.
peer	Configures a NTP peer.
server	Configures a NTP server.
<Peer IP>	IP address of the peer only.
autokey	Configures an autokey peer authentication scheme.
key	Configures a peer authentication key.
<1-65534>	Peer key number.
prefer	Prefer this peer when possible.
version	Configures NTP version.
<1-4>	NTP version number.
trusted-key	Key numbers for trusted time sources.
<1-65534>	Key number.

Example

```
RFS7000(config)#ntp peer ?
  WORD  Name/IP address of peer

RFS7000(config)#ntp peer TestPeer ?
  autokey  Configure autokey peer authentication scheme
  key      Configure peer authentication key
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

RFS7000(config)#ntp peer TestPeer autokey ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

RFS7000(config)#ntp peer TestPeer autokey prefer ?
  version  Configure NTP version
  <cr>

RFS7000(config)#ntp peer TestPeer autokey prefer version ?
  <1-4>  NTP version number

RFS7000(config)#ntp peer TestPeer autokey prefer version 3
RFS7000(config)#

RFS7000(config)#ntp peer TestPeer key ?
  <1-65534>  Peer key number

RFS7000(config)#ntp peer TestPeer key 20 ?
  prefer   Prefer this peer when possible
  version  Configure NTP version
  <cr>

RFS7000(config)#ntp peer TestPeer key 20 prefer ?
  version  Configure NTP version
  <cr>

RFS7000(config)#ntp peer TestPeer key 20 prefer version ?
  <1-4>  NTP version number

RFS7000(config)#ntp peer TestPeer key 20 prefer version 2
Invalid server name "TestPeer" provided. Please enter a valid name
RFS7000(config)#
```

5.1.23 prompt

▶ *Global Configuration Commands*

Use this command to configure and set the systems prompt.

Syntax

```
prompt(LINE)
```

Parameters

LINE	Enter the new prompt displayed by the switch.

Example

```
RFS7000(config)#prompt NobleMan
NobleMan
```

5.1.24 radius-server

▶ Global Configuration Commands

Use this CLI command to enter the RADIUS Server mode. The system prompt changes from the default config mode to RADIUS server mode.

NOTE `radius-server` **`local`** mode leads you to the radius-server context. For more details see *RADIUS Server Instance on page 13-1*

Syntax

```
radius-server(host|key|local|retransmit|timeout)
radius-server host (A.B.C.D)
radius-server key(0|2| LINE)
radius-server local
radius-server retransmit <0-100>
radius-server timeout<1-1000>
```

Parameters

host	Specifies a RADIUS server. • A.B.C.D – IP address of RADIUS server.
key	Encryption key shared with RADIUS servers. • 0 – Password specified as UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • LINE – Text of shared key (up to 127 characters in length).
local	Configures local RADIUS server parameters. This takes you to a new **`config-radius-server`** context. Refer to *RADIUS Server Instance* for more details.
retransmit <0-100>	Specifies the number of retries to the active server. • <0-100> – Number of retries for a transaction (default is 3).
timeout <1-1000>	Time to wait for a RADIUS server reply. • <1-1000> – Wait time (default 5 seconds).

Usage Guidelines

RADIUS server host is used to configure RADIUS server details. These details are required for management user authentication if AAA authentication has been defined as RADIUS.

Example

```
RFS7000(config)#radius-server local
RFS7000(config-radsrv)#
```

5.1.25 redundancy

▶ Global Configuration Commands

Use this command to configure redundancy group parameters.

Syntax

```
redundancy(discovery-period|enable|group-id|handle-stp|
heartbeat-period|hold-period|interface-ip|manual-revert|member-ip|mode)

redundancy discovery-period <10-60>
redundancy enable
redundancy group-id <1-65535>
redundancy handle-stp(enable)
redundancy heartbeat-period
redundancy hold-period <10-255>
redundancy interface-ip(A.B.C.D)
redundancy member-ip (A.B.C.D)
redundancy mode(primary|standby)
```

Parameters

discovery-period	Sets the redundancy discovery interval.
<10-60>	Discovery time in secs (default is 30).
enable	Enables the redundancy protocol.
group-id	Sets the redundancy group Id.
<1-65535>	Redundancy group Id.
handle-stp	Delays the redundancy protocol state machine exec, considering STP.
enable	Sets handle-stp value as true.
heartbeat-period	Sets the redundancy heartbeat interval.The `heartbeat-period` must always be less than the `hold-period.`
<1-255>	Heartbeat interval in secs (default is 5).
hold-period	Sets the redundancy hold interval.
<10-255>	Hold interval in secs (default is 15).
interface-ip	Sets redundancy interface IP address.
A.B.C.D	IP address of the switch.
manual-revert	Reverts standby to non-active mode.
member-ip	Add member to this redundancy group.
A.B.C.D	IP address of the member.
mode	Sets the redundancy mode.
primary	Defines mode as primary.
standby	Defines mode as standby.

Example

```
RFS7000(config)#redundancy discovery-period 20
RFS7000(config)#

RFS7000(config)#redundancy handle-stp enable
RFS7000(config)#

RFS7000(config)#redundancy heartbeat-period 20
RFS7000(config)#

RFS7000(config)#redundancy hold-period 25
RFS7000(config)#

RFS7000(config)#redundancy mode primary
RFS7000(config)#
```

5.1.26 service

▶ *Global Configuration Commands*

Use this command to retrieve system data (tables, log files, configuration, status and operation) for use in debugging and problem resolution.

Syntax

```
service(advanced-vty|dhcp|password-encryption|
pm (max-sys-restarts<1-5>|sys-restart)|
prompt(crash-info)|radius(restart)|set|show (cli)|terminal-length <0-512>)

service set ( command-history <10-300>|reboot-history <10-100>|
upgrade-history <10-100>)
```

Parameters

advanced-vty	Enables the advanced mode vty interface.
dhcp	Enables the DHCP Server.
password-encryption	Encrypts passwords.
pm (max-sys-restarts<1-5>| sys-restart)	Process Monitor. • max-sys-restarts – Maximum number of PM restarts because of a failed processes. Select a value between 1 and 5. • sys-restart – Enables PM to restart the system when a processes fails. **NOTE** The process restart is one count less than what is configured.
prompt (crash-info)	Enables crash-info prompt.
radius (restart)	Enables the RADIUS server.
set (command-history *<10-300>*| reboot-history*<10-100>*| upgrade-history*<10-100>*)	Sets service parameters. • command-history – Sets the size of the command history (default: 200). • reboot-history – Sets the size of the reboot history (default: 50). • upgrade-history – Sets the size of the upgrade history (default: 50).
show cli	Shows the CLI tree of the current mode.
terminal-length *<0-512>*	System wide terminal length configuration. Select a value between 0 - 512. This sets the number of lines of VTY (0 means no line control).

Example

```
RFS7000(config)#service dhcp
RFS7000(config)#

RFS7000(config)#service radius restart
RFS7000(config)#

RFS7000(config)#service show cli
Global Config mode:
+-aaa
  +-authentication
    +-login
      +-default
        +-local [aaa authentication login default {none|{local|radius}}]
        +-none [aaa authentication login default {none|{local|radius}}]
        +-radius [aaa authentication login default {none|{local|radius}}]
+-access-list
  +-<1-99>
    +-deny
      +-A.B.C.D/M [access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-
7> | tos <0-255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence <1-5000>
|)]
        +-log [access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p <0-7> |
tos <0-255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence <1-5000> |)]
          +-rule-precedence
            +-<1-5000> [access-list (<1-99>|<1300-1999>) (deny|permit|mark (8021p
<0-7> | tos <0-255>))(A.B.C.D/M | host A.B.C.D | any)(log|)(rule-precedence <1-
5000> |)]
        +-rule-precedence
RFS7000(config)#
```

5.1.27 show

▸ Global Configuration Commands

Use this command to view running system information.

Syntax

```
show <display parameter>
```

Parameters

access-list	Displays Internet Protocol (IP) details of the access list.
aclstats	Displays ACL statistics information.
alarm-log	Displays system alarms.
autoinstall	Displays autoinstall configuration details.
banner	Displays the “Message of the Day” login banner.
boot	Displays the boot configuration.
clock	Displays the system clock.
commands	Displays the command lists.
crypto	Displays encryption related commands.
debugging	Displays debugging information outputs.
dhcp	Displays the DHCP Server configuration.
environment	Displays environmental information.
file	Displays filesystem information.
ftp	Displays the FTP Server configuration.
history	Displays the session command history.
interfaces	Displays an interface status.
ip	Displays the Internet Protocol (IP).
ldap	Displays LDAP server.
licenses	Displays installed licenses details.
logging	Displays logging configuration and buffer data.
mac	Displays MAC access-list assignment details.
mac-address-table	Displays the MAC address table.
management	Displays L3 Managment Interface name details.
mobility	Displays mobility parameters.
ntp	Displays network time protocol.
password-encryption	Displays password encryption.

privilege	Displays current privilege level.
radius	Displays RADIUS configuration commands.
redundancy-group	Displays redundancy group parameters.
redundancy-history	Displays switch state transition history.
redundancy-members	Displays redundancy group members in detail.
running-config	Displays current operating configuration.
securitymgr	Displays securitymgr parameters.
sessions	Displays current active open connections.
snmp	Displays SNMP engine parameters.
snmp-server	Displays SNMP server parameters.
spanning-tree	Displays spanning tree information.
startup-config	Displays contents of startup configuration.
static-channel-group	Displays static channel group membership.
terminal	Displays terminal configuration parameters.
timezone	Displays timezone.
upgrade-status	Displays last image upgrade status.
users	Displays information about terminal lines.
version	Displays software and hardware version details.

Usage Guidelines

Refer to *show on page 2-25* for details of show command.

Example

```
RFS7000(config)#show ?
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  autoinstall            autoinstall configuration
  banner                 Display Message of the Day Login banner
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 Encryption related commands
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  environment            show environmental information
  file                   Display filesystem information
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                   MAC access-list assignment
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         spanning-tree Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config)#show
```

5.1.28 snmp-server

▶ Global Configuration Commands

Use this command to modify SNMP engine parameters.

Syntax

```
snmp-server(community|contact|enable|host|location|manager|sysname|user)
snmp-server community <community name>(ro|rw)
snmp-server contact LINE
snmp-server enable traps
     (all|dhcp-server|miscellaneous|mobility|
       nsm|radius-server|redundancy|snmp|wireless|wireless-statistics)

snmp-server enable traps all

snmp-server enable traps miscellaneous
(caCertExpired|lowFsSpace|processMaxRestartsReached|savedConfigModified|
 serverCertExpired)

snmp-server enable traps nsm dhcpIPChanged

snmp-server enable traps redundancy
(adoptionExceeded|grpAuthLevelChanged|memberDown|memberMisConfigured|
 memberUp)

snmp-server enable traps snmp
(authenticationFail|coldstart|linkdown|linkup)

snmp-server enable traps wireless (ap-detection|ids|radio|
self-healing|station)
snmp-server enable traps wireless  ap-detection externalAPDetected
snmp-server enable traps wireless  ids
(muExcessiveEvents|radioExcessiveEvents|switchExcessiveEvents)
snmp-server enable traps wireless radio(adopted|detectedRadar|unadopted)
snmp-server enable traps wireless self-healing activated
snmp-server enable traps wireless station
(associated|deniedAssociationAsPortCapacityReached|
deniedAssociationOnCapability|deniedAssociationOnErr|
deniedAssociationOnInvalidWPAWPA2IE|deniedAssociationOnRates|
deniedAssociationOnSSID|deniedAssociationOnShortPream|
deniedAssociationOnSpectrum|deniedAuthentication|disassociated|
radiusAuthFailed|tkipCounterMeasures)

snmp-server enable traps wireless-statistics
(min-packets|mobile-unit|radio|wireless-switch|wlan)
snmp-server enable traps wireless-statistics min-packets <1-65535>


snmp-server enable traps wireless-statistics mobile-unit
(avg-bit-speed-less-than <value>|avg-retry-greater-than <value>|
 avg-signal-less-than <value>|gave-up-percent-greater-than <value>|
 nu-percent-greater-than <value>|pktsps-greater-than <value>|
 tput-greater-than <value>|undecrypt-percent-greater-than<value>)

snmp-server enable traps wireless-statistics radio
(avg-bit-speed-less-than <value>|avg-retry-greater-than <value>|avg-signal-less-
than <value>|gave-up-percent-greater-than <value>|
nu-percent-greater-than <value>|num-mobile-units-greater-than <value>|
pktsps-greater-than <value>|tput-greater-than <value>|
undecrypt-percent-greater-than <value>)

snmp-server enable traps wireless-statistics wireless-switch
(num-mobile-units-greater-than <1-8192>|pktsps-greater-than <value>|
tput-greater-than <value>)
```

```
snmp-server enable traps wireless-statistics wlan
(avg-bit-speed-less-than|avg-retry-greater-than|avg-signal-less-than|
gave-up-percent-greater-than|nu-percent-greater-than|
num-mobile-units-greater-than|pktsps-greater-than|tput-greater-than|
undecrypt-percent-greater-than)

snmp-server host <host IP address>(v2c<1-65535>|v3<1-65535>)

snmp-server location (LINE)
snmp-server manager(all|v2|v3)
snmp-server sysname

snmp-server user(snmpmanager|snmpoperator|snmptrap)
snmp-server user (snmpmanager|snmpoperator|snmptrap) v3(auth|encrypted)
snmp-server user (snmpmanager|snmpoperator|snmptrap) v3
auth (md5<password>)
snmp-server user (snmpmanager|snmpoperator|snmptrap) v3
encrypted (auth|des)(md5<password>)
```

Parameters

(community)	Sets the community string and access privileges.
ro	Read-only access with this community string.
rw	Read-write access with this community string.
contact	Text for MIB object sysContact.
LINE	Contact person for this managed node.
enable traps ( )	Enables SNMP traps. • *all* – Enable all traps. • *dhcp-server* – Enable dhcp-server traps. • *miscellaneous* – Enable miscellaneous traps. • *mobility* – Enable mobility traps. • *nsm* – Enable nsm traps. • *radius-server* – Enable radius-server traps. • *redundancy* – Enable redundancy traps. • *snmp* – Enable SNMP traps. • *wireless* – Enable wireless traps. • *wireless-statistics* – Modify wireless-stats rate traps.
all	Enables all traps.
dhcp-server ( )	Enables dhcp-server traps. • *dhcpServerDown* – DHCP server down. • *dhcpServerUp* – DHCP server up.

miscellaneous ( )	Enables miscellaneous traps. • *caCertExpired* – Ca certificate has expired. • *lowFsSpace* – Available file system space lower than the limit. • *processMaxRestartsReached* – Process has reached the max restart limit. • *savedConfigModified* – Saved configuration has been modified. • *serverCertExpired* – Server certificate has expired.
mobility	Enables mobility traps.
nsm ( )	Enables nsm traps. • *dhcpIPChanged* – DHCP IP changed.
radius-server ( )	Enables radius-server traps. • radiusServerDown – Radius server down. • radiusServerUp – Radius server up.
redundancy ( )	Enable redundancy traps. • *adoptionExceeded* – Redundancy port adoption exceeded. • *grpAuthLevelChanged* – Redundancy group authorization level changed. • *memberDown* – Redundancy member down. • *memberMisConfigured* – Redundancy member mis-configured. • *memberUp* – Redundancy member up.
snmp ( )	Enables SNMP traps. • *authenticationFail* – Enables authentication failure traps. • *coldstart* – Enables coldStart trap. • *linkdown* – Enables linkDown trap. • *linkup* – Enables linkUp trap.
wireless ( )	Enables wireless traps. • ap-detection – Explained in the sections that follow.. • ids – Explained in the sections that follow.. • radio – Explained in the sections that follow.. • self-healing – Explained in the sections that follow.. • station – Explained in the sections that follow..
ap-detection ( )	Enables wireless access port detection traps. • *externalAPDetected* – External access port detected.

ids ( )	Enables wireless IDS traps. • muExcessiveEvents – Excessive MU events. • radioExcessiveEvents – Excessive radio events. • switchExcessiveEvents – Excessive switch events.
radio ( )	Enables wireless radio traps. • *adopted* – Radio adopted. • *detectedRadar* – Radio detected radar. • *unadopted* – Radio unadopted.
self-healing ( )	Enables self healing traps. • *activated* – Self healing activated.
station ( )	Wireless station traps. • *associated* – Denied association due to port capacity reached. • *deniedAssociationAsPortCapacityReached* – Denied association due to reached port capacity. • *deniedAssociationOnCapability* – Denied association due to unsupported capability. • *deniedAssociationOnErr* – Denied association due to internal error. • deniedAssociationOnInvalidWPAWPA2IE – Denied association due to invalid/absent WPA/WPA2 IE. • *deniedAssociationOnRates* – Denied association due to incompatible transmission rate. • deniedAssociationOnSSID – Denied association due to invalid SSID. • deniedAssociationOnShortPream – Denied association due to lack of short preamble support. • *deniedAssociationOnSpectrum* – Denied association due to lack of spectrum management capability. • *deniedAuthentication* – Denied 802.11 authentication. • *disassociated* – Disassociated. • *radiusAuthFailed* – Failed radius authentication. • *tkipCounterMeasures* – TKIP counter measures invoked.–

wireless-statistics ( )	Modifies wireless-stats rate traps. • min-packets– Explained in the sections that follow. • mobile-unit– Explained in the sections that follow. • radio– Explained in the sections that follow. • wireless-switch– Explained in the sections that follow. • wlan– Explained in the sections that follow.
min-packets <1-65535>	Minimum packets for sending the trap. Set with a decimal number in the range of <1-65535>.
mobile-unit	Modifies mobile unit rate traps. • *avg-bit-speed-less-than <value>*– Average bit speed in Mbps is less than *<a decimal number greater than 0.00 and less than or equal to 54.00>.* • *avg-retry-greater-than <value>* – Average retry is greater than *<a decimal number greater than 0.00 and less than or equal to 16.00>.* • *avg-signal-less-than <value>* – Average signal in dBm is less than *< a decimal number less than -0.00 and greater than or equal to -120.00>.* • *gave-up-percent-greater-than <value>* – Percentage of pkts dropped is greater than *< a decimal number greater than 0.00 and less than or equal to 100.00>.* • *nu-percent-greater-than <value>*– Percentage of non-unicast pkts is greater than *< a decimal number greater than 0.00 and less than or equal to 100.00>.* • *pktsps-greater-than <value>*– Packets per sec is greather than *< a decimal number greater than 0.00 and less than or equal to 100000.00>.* • *tput-greater-than <value>*– Throughput in Mbps is greather than *< a decimal number greater than 0.00 and less than or equal to 100000.00>.* • *undecrypt-percent-greater-than <value>*– Percentage of undecryptable pkts is geater than *< a decimal number greater than 0.00 and less than or equal to 100.00>.*

radio	Modifies radio rate traps. • *avg-bit-speed-less-than <value>*– Average bit speed in Mbps is less than *<a decimal number greater than 0.00 and less than or equal to 54.00>.* • *avg-retry-greater-than <value>* – Average retry is greater than *<a decimal number greater than 0.00 and less than or equal to 16.00>.* • *avg-signal-less-than <value>* – Average signal in dBm is less than *< a decimal number less than -0.00 and greater than or equal to -120.00>.* • *gave-up-percent-greater-than <value>* – Percentage of pkts dropped is greater than *< a decimal number greater than 0.00 and less than or equal to 100.00>.* • *nu-percent-greater-than <value>*– Percentage of non-unicast pkts is greater than *< a decimal number greater than 0.00 and less than or equal to 100.00>.* • *num-mobile-units-greater-than <1-8192>* – Number of associated mobile unit is greater than < a decimal number in the range <1-8192>. • *pktsps-greater-than <value>*– Packets per sec is greather than *< a decimal number greater than 0.00 and less than or equal to 100000.00>.* • *tput-greater-than <value>*– Throughput in Mbps is greather than *< a decimal number greater than 0.00 and less than or equal to 100000.00>.*
	• *undecrypt-percent-greater-than <value>*– Percentage of undecryptable pkts is geater than *< a decimal number greater than 0.00 and less than or equal to 100.00>.*

wireless-switch	Modify wireless-switch rate traps. • *num-mobile-units-greater-than <1-8192>* – Number of associated MUs is greater than *<a decimal number in the range 1-8192 >.* • *pktsps-greater-than <value>* – Packets per sec is greather than *<a decimal number greater than 0.00 and less than or equal to 100000.00>.* • *tput-greater-than <value>* – Throughput in Mbps is greather than *< a decimal number greater than 0.00 and less than or equal to 100000.00>.*
wireless-statistics wlan ( )	Modify WLAN rate traps. • avg-bit-speed-less-than < value> – Average bit speed in Mbps is less than <a decimal number greater than 0.00 and less than or equal to 54.00>. • avg-retry-greater-than <*value* > – Average retry is greater than *< a decimal number greater than 0.00 and less than or equal to 16.00>.* • avg-signal-less-than < value> – Average signal in dBm is less than <a decimal number less than -0.00 and greater than or equal to -120.00>. • gave-up-percent-greater-than <*value* > – Percentage of pkts dropped is greater than *<a decimal number greater than 0.00 and less than or equal to 100.00>.* • nu-percent-greater-than <value> – Percentage of non-unicast pkts is greater than <a decimal number greater than 0.00 and less than or equal to 100.00>. • pktsps-greater-than <value> – Packets per sec is greather than <a decimal number greater than 0.00 and less than or equal to 100000.00>. • tput-greater-than <*value*> – Throughput in Mbps is greather than *<a decimal number greater than 0.00 and less than or equal to 100000.00>.* • *undecrypt-percent-greater-than <value >* – percentage of undecryptable pkts is geater than *<a decimal number greater than 0.00 and less than or equal to 100.00>.* • num-mobile-units-greater-than <1-4096 > – Number of associated MUs is greater than a number within the range of <1-4096>.

host <host IP address>	SNMP server host IP-address.
v2c <1-65535>	Uses SNMP version 2c. Select a host port number within the range of <1-65535>.
v3 <1-65535>	Uses SNMP version 3. Select a host port number within the range of <1-65535>.
location	Text for mib object sysLocation.
manager	Enables SNMP manager.
all	Enables SNMP version v2 and v3.
v2	Enables SNMP version v2.
v3	Enables SNMP version v3.
sysname	SNMP system name.
user	Definse a user who can access the SNMP engine.
snmpmanager	Manager user.
snmpoperator	Operator user.
snmptrap	Trap user.
v3 ( )	User currently uses a v3 security model.
auth ( )	Authentication parameters for the user.
encrypted ( )	Specifies password as md5 digests.
md5	Uses HMAC MD5 algorithm for authentication.
des	Uses CBC-DES for privacy.
PASSWD	Authentication password for user.

Example

```
RFS7000(config)#snmp-server community TestCommunity ro
RFS7000(config)#

RFS7000(config)#snmp-server contact TestManager
RFS7000(config)#

RFS7000(config)#snmp-server enable traps all
RFS7000(config)#

RFS7000(config)#snmp-server enable traps miscellaneous lowFsSpace
RFS7000(config)#

RFS7000(config)#snmp-server enable traps redundancy memberUp
RFS7000(config)#

RFS7000(config)#snmp-server enable traps snmp linkup
RFS7000(config)#

RFS7000(config)#snmp-server enable traps wireless  ap-detection
externalAPDetected
```

```
RFS7000(config)#

RFS7000(config)#snmp-server enable traps wireless  ids excessiveProbes
RFS7000(config)#

RFS7000(config)#snmp-server enable traps wireless radio adopted
RFS7000(config)#

RFS7000(config)#snmp-server enable traps wireless self-healing activated
RFS7000(config)#

RFS7000(config)#snmp-server enable traps wireless station tkipCounterMeasures
RFS7000(config)#

RFS7000(config)#snmp-server enable traps wireless-statistics min-packets 120
RFS7000(config)#

RFS7000(config)#snmp-server location "Located at thh 5th FLoor"
RFS7000(config)#

RFS7000(config)#snmp-server sysname "Gold Mine"
RFS7000(config)#
```

5.1.29 spanning-tree

▶ *Global Configuration Commands*

Use this command to configure the spanning-tree commands.

Syntax

```
spanning-tree [mst|portfast]

spanning-tree mst [<0-15> (priority <0-61440>)|
cisco-interoperability (enale|disable)|configuration|
forward-time <4-30>|hello-time <1-10>|max-age <6-40>|max-hops <7-127>]

spanning-tree portfast [bpdufilter|bpduguard](default)
```

Parameters

mst [<0-15> (priority <0-61440>)| cisco-interoperability (enale|disable)| configuration| forward-time <4-30>| hello-time <1-10>| max-age <6-40>| max-hops <7-127>]	Enables the Multiple Spanning Tree Protocol on a bridge. • <0-15> (priority <0-61440>) – Set the bridge priority for an MST instance to the value specified. Use the `no` parameter with this command to restore the default bridge priority value. • priority – Bridge priority for the common instance. • <0-61440> – Bridge priority in increments of 4096 (Lower priority indicates greater likelihood of becoming root). The default value of the priority for each instance is `32768`. • cisco-interoperability (enale|disable) – Enables/disables interoperability with Cisco's version of MSTP (incompatible with standard MSTP). • enable – Enables CISCO Interoperability. • disable – Disables CISCO Interoperability. • configuration – Multiple spanning tree configuration. This command moves to the *spanning tree-mst Instance* instance.

	• forward-time <4-30> – Sets the time (in seconds) after which (if this bridge is the root bridge) each port changes states to learning and forwarding. This value is used by all instances. The default value is 15 seconds. • hello-time <1-10> – Sets the hello-time. The hello-time is the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange *Bridge Protocol Data Units* (BPDUs). A very low value leads to excessive traffic on the network, while a higher value delays the detection of topology change. This value is used by all instances. The default value is 2 seconds. • max-age <6-40> – Max-age is the maximum time in seconds for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. The value of max-age must be greater than twice the value of hello time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the max-age. Use this command to set the max-age for a bridge. This value is used by all instances. The default value of bridge max-age is 20 seconds. • max-hops <7-127> – Specifies the maximum allowed hops for a BPDU in an MST region. This parameter is used by all MST instances. To restore the default value, use the no parameter with this command. The default max-hops in a MST region is 20.
portfast [bpdufilter|bpduguard](default)	Enables the portfast feature on a bridge. It has the following options: • bpdufilter (default) – Use the `bpdu-filter` command to set the portfast BPDU filter for the port. Use the no parameter with this command to revert the port BPDU filter value to default. The Spanning Tree Protocol sends BPDUs from all ports. Enabling the BPDU Filter feature ensures PortFastenabled ports do not transmit or receive BPDUs. • bpduguard (default) – Use the `bpdu-guard` command to enable the BPDU (Bridge Protocol Data Unit) Guard feature on a bridge. Use the `no` parameter with this command to disable BPDU Guard. When the BPDU Guard is set for a bridge, all portfast-enabled ports of the bridge that have bpdu guard set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed. The port can be brought back up manually (using the no shutdown command), or by configuring a errdisable-timeout to enable the port after the specified interval.

Usage Guidelines

The `mst > configuration` command moves you to the *spanning tree-mst Instance* instance.

If a bridge does not hear *bridge protocol data units* (BPDUs) from the root bridge within the specified interval, defined in the max-age (seconds) parameter, then assume that the network has changed and recompute the spanning-tree topology.

Generally spanning tree configuration settings in config mode does the configuration for bridge and bridge instances (for the switch).

Example

```
RFS7000(config)*#spanning-tree portfast bpduguard default
RFS7000(config)*#
```

5.1.30 timezone

▶ *Global Configuration Commands*

Use this command to configure switch timezone settings.

Syntax

```
timezone
```

Parameters

TIMEZONE	Press <tab> to navigate the list of files. This action displays a list of files containing timezone information.

Example

```
RFS7000(config)#timezone
Africa/     America/   Asia/      Atlantic/  Australia/  Etc/       Europe/
Pacific/
RFS7000(config)#timezone

RFS7000(config)#timezone America/
America/Anchorage   America/Bogota      America/Buenos_Aires America/Caracas
America/Chicago
America/Costa_Rica    America/Denver        America/Los_Angeles   America/
Mexico_City   America/Montreal
America/New_York      America/Phoenix       America/Santiago      America/
Sao_Paulo     America/St_Johns
America/Tegucigalpa   America/Thule         America/Winnipeg      America/
Indianapolis

RFS7000(config)#timezone America/Chicago
RFS7000(config)#
```

5.1.31 username

- *Global Configuration Commands*

Use this CLI command to establish the user name authentication.

Syntax

```
username <name> (access|password|privilege)
username <name> access (console|ssh|telnet|web)
username <name> password(0|1|Line)
username <name> privilege(helpdesk|monitor|nwadmin|superuser|sysadmin|webadmin)
```

Parameters

name	Enter a name to authenticate the switch. The username must be between 1 - 28 characters.
access	Sets the user access mode. • console – Only allowed from console. • ssh – Only allowed from ssh. • telnet – Only allowed from telnet. • web – Only allowed from applet (webUI).
password	Specifies the user password. • 0– Password is specified UNENCRYPTED. • 1– Password is encrypted with SHA1 algorithm. • LINE– User password (plaintext passsword length must be between 8 and 32 characters).
privilege	Sets user access privileges. • helpdesk – Helpdesk (troubleshooting) access. • monitor – Monitor (read-only) access. • nwadmin – Network (wired & wireless) admin access. • superuser – Superuser (root) access. • sysadmin – System (general system configuration) admin access. • webadmin – Web auth (hotspot) user admin access.

Example

```
RFS7000(config)#username GoldenSwitch
RFS7000(config)#
```

5.1.32 wireless

▶ *Global Configuration Commands*

Use this command to configure switch wireless parameters. This command leads moves you to the `config-wireless` instance. For additional information, see *Wireless Instance on page 14-1*.

Syntax

```
wireless
```

Parameters

None.

Usage Guidelines

The wireless command is used to enter the config-wireless instance. The prompt changes from the regular `RFS7000(config)#` to `RFS7000(config-wireless)#.`

Example

```
RFS7000(config)#wireless
RFS7000(config-wireless)#
```

5.1.33 wlan-acl

▶ *Global Configuration Commands*

Use this command to apply an ACL on a WLAN index.

Syntax

```
wlan-acl [<1-256>{<1-99>|<100-199>|<1300|1999>|<2000|2699>|word}][in|out]
```

Parameters

<1-256>[]	WLAN number. • <1-99> — IP standard access list. • <100-199> — IP extended access list. • <1300-1999> — IP standard access list (expanded range). • <2000-2699> — IP extended access list (expanded range). • WORD — Access list name.

Usage Guidelines

Every WLAN created is mapped to an index. When an ACL is applied on a WLAN index it becomes a WLAN ACL. The following type of ACL's can be applied on a WLAN:

- IP Standard ACL
- IP Extended ACL
- MAC Extended ACL

When a packet is send from a client to a WLAN index of an access port, it becomes an inbound traffic to the wireless LAN.

When a packet goes out of a access port, it becomes a outbound traffic to the wireless LAN index. Apply an ACL to a WLAN index in outbound direction to filter traffic from both wired and wireless interfaces.

`wlan-acl` can be attached both in the inbound and outbound directions.

NOTE Most of the Wireless LAN related configuration are performed using the *Wireless Instance on page 14-1*.

Use `wlan-acl` (in the global configuration mode) to apply an ACL on a wireless LAN index .

The last ACE in the access list is an implict deny statement. Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed/denied based on the ACL configuration.

Example

The example below applies an ACL to WLAN index 200 in inbound direction from the global config mode.

```
RFS7000(config)#wlan-acl 200 150 in
RFS7000(config)#
```

NOTE A MAC access list entry to allow `arp` is mandatory to apply an IP based ACL to an interface. MAC ACL always takes precedence over IP based ACL's.

The example below applies an ACL to WLAN index 200 in outbound direction from the global config mode.

```
RFS7000(config)#wlan-acl 200 150 out
RFS7000(config)#
```

crypto-trustpoint Instance

Use `config-crypto-trustpoint` commands to define a *Certificate Authority* (CA) trustpoint. `config-crypto-trustpoint` is a seperate instance, belonging to the `crypto pki trustpoint` mode under the `config` instance.

6.1 Trustpoint Config commands

Table 6.1 summarizes the **`config-crypto-trustpoint`** commands.

Table 6.1 Trustpoint Config Commands Summary

Command	***Description***	***Ref.***
clrscr	Clears the display screen.	page 6-3
company-name	Company name (applicable only for request).	page 6-4
email	Email.	page 6-5
end	Ends the current mode and moves to the EXEC mode.	page 6-6
exit	Ends the current mode and moves to the previous mode.	page 6-7
fqdn	Domain name configuration.	page 6-8
help	Describes the interactive help system.	page 6-9
ip-address	Internet Protocol (IP).	page 6-10
no	Negates a command or set defaults.	page 6-11

Command	Description	Ref.
password	Challenge password (appplicable only by request).	page 6-12
rsakeypair	Rsa Keypair to associate with the trustpoint.	page 6-13
service	Service commands.	page 6-14
show	Shows the running system information.	page 6-15
subject-name	Subject name is a collection of required parameters to configure a trustpoint. It consists of the common_name, country, state, organization, org, name, etc.	page 6-17

6.1.1 clrscr

▶ *Trustpoint Config commands*

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-trustpoint)#clrscr
RFS7000(config-trustpoint)#
```

6.1.2 company-name

▸ Trustpoint Config commands

Use this command to set the company name (applicable only by request) to a trustpoint.

Syntax

```
company-name
```

Parameters

WORD	Company name (2 - 64 characters in length).

Usage Guidelines

The company name defined must be in the range of 2 to 64 characters only.

Example

```
RFS7000(config-trustpoint)#company-name RetailKing
RFS7000(config-trustpoint)#
```

6.1.3 email

▶ *Trustpoint Config commands*

Use this command to configure an e-mail ID for a trustpoint.

Syntax

```
email
```

Parameters

WORD	email address (2 to 64 characters).

Usage Guidelines

The email defined must be in the range of 2 to 64 characters only.

Example

```
RFS7000(config-trustpoint)#email abcTestemailID@motorola.com
RFS7000(config-trustpoint)#
```

6.1.4 end

▶ *Trustpoint Config commands*

Use this command to end and exit the current mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#.`

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-trustpoint)#end
RFS7000#
```

6.1.5 exit

▸ *Trustpoint Config commands*

Use this command to end the current mode and down to previous mode (GLOBAL-CONFIG). The prompt now changes to `RFS7000(config)#.`

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-trustpoint)#exit
RFS7000(config)#
```

6.1.6 fqdn

▶ *Trustpoint Config commands*

Use this command to configure the *fully qualified domain name* (fqdn) for the trustpoint.

Syntax

```
fqdn
```

Parameters

None

Usage Guidelines

The string length of the domain name must between 9 to 64 characters.

Example

```
RFS7000(config-trustpoint)#fqdn RetailKing.com
RFS7000(config-trustpoint)#
```

6.1.7 help

▶ *Trustpoint Config commands*

Use this command to access the system’s interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-trustpoint)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-trustpoint)#
```

6.1.8 ip-address

▶ *Trustpoint Config commands*

Use this command to configure an IP address for the trustpoint.

Syntax

```
ip-address
```

Parameters

A.B.C.D	Enter the IP address configured for the trustpoint.

Example

```
RFS7000(config-trustpoint)#ip-address 157.200.200.02
RFS7000(config-trustpoint)#
```

6.1.9 no

▶ *Trustpoint Config commands*

Use this command to negate a command or set defaults.

Syntax

```
no <previous command used>
```

Parameters

None.

Example

```
RFS7000(config-trustpoint)#no ip-address
RFS7000(config-trustpoint)#
```

6.1.10 password

▶ *Trustpoint Config commands*

Use this command to set the challenge password, applicable only for trustpoint access requests .

Syntax

```
password(0|2|WORD)
```

Parameters

0	Password is specified UNENCRYPTED. The password must be between 4 - 20 characters.
2	Password is encrypted with a password-encryption secret. The string length of an encrypted password must be between 44 - 64 characters.
WORD	Password (4 - 20 characters).

Example

```
RFS7000(config-trustpoint)#password 0 TestPassword
RFS7000(config-trustpoint)#
```

6.1.11 rsakeypair

▶ *Trustpoint Config commands*

Use this command to configure a RSA Keypair to associate with the trustpoint.

Syntax

```
rsakeypair
```

Parameters

WORD	RSA keypair identifier.

Usage Guidelines

Use RSA Key Pair support to configure the switch to have *Rivest, Shamir, and Adelman* (RSA) key pairs. The switch software can maintain a different key pair for each identity certificate.

Example

```
RFS7000(config-trustpoint)#rsakeypair were
RFS7000(config-trustpoint)#
```

The `rsakeypair` name `were` in this example is an exisitng keypair value.

6.1.12 service

Trustpoint Config commands

Use this command to invoke service commands to trobuleshoot or debug `crypto pki trustpoint` instance configurations.

Syntax

```
service(show)(cli)
```

Parameters

show (cli)	Shows the CLI tree of current mode.

Example

```
RFS7000(config-trustpoint)#service show cli
Trustpoint Config mode:
+-clrscr [clrscr]
+-company-name
  +-WORD [company-name WORD]
+-do
  +-LINE [do LINE]
+-email
  +-WORD [email WORD]
+-end [end]
+-exit [exit]
+-fqdn
  +-WORD [fqdn WORD]
+-help [help]
+-ip-address
  +-A.B.C.D [ip-address A.B.C.D]
+-no
  +-company-name [no company-name]
  +-email [no email]
  +-fqdn [no fqdn]
  +-ip-address [no ip-address]
  +-subject-name [no subject-name]
+-password
  +-0
    +-WORD [password (0|2|) WORD]
  +-2
    +-WORD [password (0|2|) WORD]
  +-WORD [password (0|2|) WORD]
+-quit [quit]
+-rsakey
  +-WORD [rsakey WORD]
+-rsakeypair
  +-WORD [rsakeypair WORD]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
+-service
  +-show
.................................................................................
.................................................................................
.................................................................................
.................................................................................
....

RFS7000(config-trustpoint)#
```

6.1.13 show

▶ *Trustpoint Config commands*

Use this command to view current system information.

Syntax

```
show <parameter>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Example

```
RFS7000(config-trustpoint)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                Encryption related commands
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   MAC access-list assignment
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         spanning-tree Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
```

```
RFS7000(config)#show crypto pki trustpoints

Trustpoint :default-trustpoint
-----------------------------------------------
  Server certificate configured
    Subject Name:
      Common Name:         Symbol Technologies
    Issuer Name:
      Common Name:         Symbol Technologies
  Valid From:   Mar 11 03:38:26 2007 GMT
  Valid Until:  Mar 10 03:38:26 2008 GMT
RFS7000(config)#
```

```
RFS7000(config-trustpoint)#show access-list
Standard IP access list 1
    deny any rule-precedence 1
RFS7000(config-trustpoint)#
```

```
RFS7000(config-trustpoint)#show sessions
SESSION   USER       LOCATION        IDLE         START TIME
   1       cli    Console           06:12m      Jan  1 00:00:00 1970
** 2       cli    157.235.206.39    00:00m      Jan  1 00:00:00 1970
RFS7000(config-trustpoint)#
```

```
RFS7000(config-trustpoint)#show users
   Line       PID   User        Uptime      Location
   0 con 0  306               06:14:07     ttyS0
 130 vty 0  2744               00:25:49     0
RFS7000(config-trustpoint)#
```

```
RFS7000(config-trustpoint)#show upgrade-status
Last Image Upgrade Status : Successful
Last Image Upgrade Time   : Tue Aug 29 18:32:17 2006
RFS7000(config-trustpoint)#
```

6.1.14 subject-name

▶ *Trustpoint Config commands*

Use this command to create a subject name in order to configure a trustpoint. A subject name is a collection of required parameters.

Syntax

```
subject-name
```

Parameters

WORD	The subject name is a collection of required parameters to configure a trustpoint. It consists of the common_name, country, state, org name etc.

Example

```
RFS7000(config-trustpoint)#subject-name TestPool ?
  WORD  Country ( 2 character ISO Code )

RFS7000(config-trustpoint)#subject-name TestPool US ?
  WORD  State( 2 to 128 characters )

RFS7000(config-trustpoint)#subject-name TestPool US OH ?
  WORD  City( 2 to 128 characters )

RFS7000(config-trustpoint)#subject-name TestPool US OH PB ?
  WORD  Organization( 2 to 64 characters )

RFS7000(config-trustpoint)#subject-name TestPool US OH PB MOTOROLA ?
  WORD  Organization Unit( 2 to 64 characters )

RFS7000(config-trustpoint)#subject-name TestPool US OH PB MOTOROLA WID ?
  <cr>

RFS7000(config-trustpoint)#subject-name TestPool US OH PB MOTOORLA WID
RFS7000(config-trustpoint)#
```

7

interface Instance

Use the **(config-if**) instance to configure Fast Ethernet (fe), Giga Ehternet (ge), StaticAggregate interface (sa), VLAN and tunnel . Use the `(config)# interface [fe|ge|sa|tunnel|vlan]` to reach this instance.

7.1 Interface Config commands

Table 7.1 summarizes the **config-if** commands.

Table 7.1 Interface Config Command Summary

Command	**Description**	**Ref.**
clrscr	Clears the display screen.	page 7-3
description	Interface specific description.	page 7-4
duplex	Sets the duplex to interface.	page 7-5
end	Ends the current mode and moves to the EXEC mode.	page 7-6
exit	Ends the current mode and moves down to the previous mode.	page 7-7
help	Describes the interactive help system.	page 7-8
ip	Internet Protocol (IP).	page 7-9
mac	MAC interface commands.	page 7-11
management	Sets the selected interface as the management interface.	page 7-12
mtu	Sets the mtu value for the VLAN interface.	page 7-13
no	Negates a command or sets defaults.	page 7-14

Command	Description	Ref.
port-channel	Port channel commands.	page 7-15
service	Service commands.	page 7-16
show	Shows the running system information.	page 7-17
shutdown	Shutsdown the selected interface.	page 7-20
spanning-tree	Configures spanning-tree.	page 7-21
speed	Configures speed.	page 7-23
static-channel-group	Configures static channel commands.	page 7-24
switchport	Sets switching mode characteristics.	page 7-25
tunnel	Protocol-over-protocol tunneling.	page 7-27

7.1.1 clrscr

▶ *Interface Config commands*

Use this command to clear the screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-if)#clrscr
RFS7000(config-if)#
```

7.1.2 description

▶ *Interface Config commands*

Use this command to create an interface specific desciption.

Syntax

```
description
```

Parameters

LINE	Characters to describe this interface.

Example

```
RFS7000(config-if)#description "interface for RetailKing"
RFS7000(config-if)#
```

7.1.3 duplex

▶ *Interface Config commands*

Use this command to configure a duplex type for the interface.

NOTE

- Duplexity can only be set for an Ethernet type interface. Enter the `(config-if)` instance using an `ge/me` parameter in an `interface` mode.
- Duplex cannot be set until the speed is set to a non-auto value.

Syntax

```
duplex(auto|full|half)
```

Parameters

auto	Sets the auto-negotiate parameter.
full	Sets full-duplex where data can be passed in both direction simultaneoulsy.
half	Sets half-duplex where data can only be passed in one direction at a time.

Usage Guidelines

Duplex defines the type of communication used by the port. The switch, by default, is set as `auto` duplex. In auto mode the duplex is selected based on the connected network hardware.

Example

```
RFS7000(config)#interface ge4

RFS7000(config-if)#duplex ?
  auto  set auto-negotiate
  full  set full-duplex
  half  set half-duplex

RFS7000(config-if)#duplex full
RFS7000(config-if)#
```

7.1.4 end

▶ *Interface Config commands*

Use this command to exit from the current mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-if)#end
RFS7000#
```

7.1.5 exit

Interface Config commands

Use this command to end the current mode and move down to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-if)#exit
RFS7000(config)#
```

7.1.6 help

▶ *Interface Config commands*

Use this command to access the system’s interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-if)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-if)#
```

7.1.7 ip

▸ *Interface Config commands*

Use this command to configure an IP address for the assigned Ethernet, VLAN or tunnel.

Syntax

```
ip(access-group|address|helper-address|nat)
ip access-group(<1-99>|<100-199>|<1300-1999>|<2000-2699>)in
ip address(A.B.C.D/M|dhcp)
ip helper-address A.B.C.D
ip nat(inside|outside)
```

Parameters

access-group	Access group.
(<*1-99*> |<*100-199*>)	IP extended access list.
(<*1300-1999*>|<*2000-2699*>)	IP extended access list (expanded range).
WORD	Access list name.
in	Incoming packets.
address	Sets the interface IP address.
A.B.C.D/M	IP address (for example, 10.0.0.1/8).
dhcp	Uses a DHCP Client to obtain an IP address for the interface.
helper-address	Forwards DHCP and BOOTP packets.
A.B.C.D	IP to which DHCP and BOOTP packets are forwarded.
nat	*Network Address Translation* (NAT).
inside	Inside interface.
outside	Outside interface.

Usage Guidelines

IPv4 commands are not allowed on a L2 interface. Use the `ip access-group` command to attach an access list to an interface. Use the `no ip access-group` command to remove the access list from the interface.

Use `mac access-group` to atach a MAC access list to an interface.

Example

```
RFS7000(config-if)#ip access-group 110 in
RFS7000(config-if)#

RFS7000(config-if)#ip address 192.168.234.1/24
RFS7000(config-if)#
```

Follow the steps in the example below to create a helper address on VLAN 2000 for using the DHCP server available on VLAN 1000.

```
RFS7000(config)#interface vlan 1000
RFS7000(config-if)#ip address 172.168.100.1/24
```

```
RFS7000(config-if)#interface vlan 2000
RFS7000(config-if)#ip address 172.168.200.1/24

RFS7000(config-if)#ip helper-address 172.168.100.10 vlan 1000
RFS7000(config-if)#
```

The example below displays static NAT source translation.

```
RFS7000(config)#interface vlan 1000
RFS7000(config-if)#ip nat inside

RFS7000(config-if)#interface vlan 2000
RFS7000(config-if)#ip nat outside

RFS7000(config)#ip nat inside source static 172.168.200.10 157.235.205.57
RFS7000(config)#
```

7.1.8 mac

▶ *Interface Config commands*

Use this command to apply a MAC access list to a gigabit ethernet interface.

✓ **NOTE** Access list cannot be appllied on a management interface (me1).

Syntax

```
mac (access-group <acl_name>) (in)
```

Parameters

access-group <acl_name>	Sets MAC access groups ACL.
in	Apply the ACL to ingress packets.

Example

```
RFS7000(config-if)#mac access-group Ark200 in
RFS7000(config-if)#
```

7.1.9 management

▶ *Interface Config commands*

Use this command to configure the selected interface as a management interface.

Syntax

```
management
```

Parameters

None.

Usage Guidelines

Management privilage can be set only on a L3 interface. Use this command along with the `(config) management secure` in config mode. This ensure management access of the switch is restricted to the management VLAN only.

Refer *management on page 5-35* for `(config) management secure` configuration.

Example

```
RFS7000(config)#interface vlan 1000
RFS7000(config-if)#management
RFS7000(config-if)#
```

7.1.10 mtu

▶ *Interface Config commands*

Use this command to set the mtu value for a VLAN interface.

NOTE This command is valid only with a VLAN interface.

Syntax

```
mtu <512-1500>
```

Parameters

<512-1500>	Maximum packet size in bytes. The minimum value is 512 and maximum value is 1500.

Usage Guidelines

All interfaces have a default maximum packet size of 1500 bytes. Use the `mtu` command to set the MTU size of the packets thats travels through the interface.

Example

```
RFS7000(config)#interface vlan 20

RFS7000(config-if)#mtu 520
RFS7000(config-if)#
```

7.1.11 no

Interface Config commands

Use this command to negate a command or set defaults.

Syntax

```
no [description|duplex|ip|mtu|shutdown|
    spanning-tree|speed|static-channel-group|switchport|tunnel]
```

Parameters

The `no` command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFS7000(config-if)#no mtu
RFS7000(config-if)#

RFS7000(config-if)#no spanning-tree link-type
RFS7000(config-if)#

RFS7000(config-if)#no spanning-tree portfast
RFS7000(config-if)#

RFS7000(config-if)#no spanning-tree portfast bpdu-guard
RFS7000(config-if)#

RFS7000(config-if)#no spanning-tree portfast bpdu-filter
RFS7000(config-if)#
```

7.1.12 port-channel

▶ *Interface Config commands*

Use this command to select the load-balance criteria of a aggregated port. This command

Syntax

```
port-channel (load-balance [src-dst-ip|src-dst-mac])
```

Parameters

load-balance [src-dst-ip|src-dst-mac]	Sets load-balancing for port channel. • src-dst-ip – Source and Destination IP address based load balancing. • src-dst-mac – Source and Destination MAC address based load balancing

Usage Guidelines

Use this command to configure and set the load balance to the aggregated port created using `(config-if) static-channel-group`.

Example

The example below creates a channel group 1 with interface ge1 and ge 2.

```
RFS7000(config)#interface ge1
RFS7000(config-if)#static-channel-group 1

RFS7000(config)#interface ge2
RFS7000(config-if)#static-channel-group 1
```

The example beow select the load balance based on IP or MAC address.

```
RFS7000(config)#interface sa1
RFS7000(config-if)#port-channel load-balance src--dst-ip
RFS7000(config-if)#
```

7.1.13 service

▶ Interface Config commands

Use this command to invoke service commands to trobuleshoot or debug the `(config-if)` instance configurations.

Syntax

```
service(show) (cli)
```

Parameters

show	Shows running system information.
cli	Shows the CLI tree of current mode.

Example

```
RFS7000(config-if)#service show cli
Interface Config mode:
+-cisco-interoperability
  +-disable [cisco-interoperability ( enable | disable)]
  +-enable [cisco-interoperability ( enable | disable)]
+-clrscr [clrscr]
+-description
  +-LINE [description LINE]
+-do
  +-LINE [do LINE]
+-duplex
  +-auto [duplex (half|full|auto)]
  +-full [duplex (half|full|auto)]
  +-half [duplex (half|full|auto)]
+-end [end]
+-exit [exit]
+-help [help]
+-ip
  +-access-group
    +-<1-99>
      +-in [ip access-group (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD) (in)]
    +-<100-199>
      +-in [ip access-group (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD) (in)]
    +-<1300-1999>
      +-in [ip access-group (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD) (in)]
    +-<2000-2699>
      +-in [ip access-group (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD) (in)]
    +-WORD
      +-in [ip access-group (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)
(in)]...................................................................
........................................................................
........................................................................
........................................................................
.............................................
RFS7000(config-if)#
```

7.1.14 show

▶ *Interface Config commands*

Use this command to view current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Example

```
RFS7000(config-if)#show ?
  access-list            Internet Protocol (IP)
  aclstats               Show ACL Statistics information
  alarm-log              Display all alarms currently in the system
  autoinstall            autoinstall configuration
  banner                 Display Message of the Day Login banner
  boot                   Display boot configuration.
  clock                  Display system clock
  commands               Show command lists
  crypto                 Encryption related commands
  debugging              Debugging information outputs
  dhcp                   DHCP Server Configuration
  file                   Display filesystem information
  ftp                    Display FTP Server configuration
  history                Display the session command history
  interfaces             Interface status
  ip                     Internet Protocol (IP)
  ldap                   LDAP server
  licenses               Show any installed licenses
  logging                Show logging configuration and buffer
  mac                    MAC access-list assignment
  management             Display L3 Managment Interface name
  mobility               Display Mobility Parameters
  ntp                    Network time protocol
  password-encryption    password encryption
  privilege              Show current privilege level
  radius                 RADIUS configuration commands
  redundancy-group       Display redundancy group parameters
  redundancy-history     Display state transition history of the switch.
  redundancy-members     Display redundancy group members in detail
  running-config         Current Operating configuration
  securitymgr            Securitymgr parameters
  sessions               Display current active open connections
  snmp                   Display SNMP engine parameters
  snmp-server            Display SNMP engine parameters
  spanning-tree          spanning-tree Display spanning tree information
  startup-config         Contents of startup configuration
  static-channel-group   static channel group membership
  terminal               Display terminal configuration parameters
  timezone               Display timezone
  upgrade-status         Display last image upgrade status
  users                  Display information about terminal lines
  version                Display software & hardware version
  wireless               Wireless configuration commands
  wlan-acl               wlan based acl

RFS7000(config-if)#show
```

```
RFS7000(config-if)#show boot

Image           Build Date              Install Date           Version
-----       --------------------    --------------------     --------------
Primary     Aug 28 14:05:16 2006     Aug 29 18:32:17 2006     3.0.0.0-200B
Secondary   Aug 14 06:18:03 2006     Aug 17 15:08:28 2006     3.0.0.0-180B

Current Boot       : Primary
Next Boot          : Primary
Software Fallback  : Enabled
RFS7000(config-if)#

RFS7000(config-if)#show wireless ?
  ap                          Status of adopted access-port
  ap-detection-config         Detected-AP Configuration Parameters
  ap-images                   List of access-port images on the wireless
                              switch
  ap-unadopted                List of unadopted access-port
  approved-aps                Approved APs seen by access-port scans
  channel-power               List of available channel and power levels for
                              a radio
  config                      Wireless Configuration Parameters
  hotspot-config              Wlan hotspot configuration
  ids                         Intrusion detection parameters
  mac-auth-local              list out the mac-auth-local entries
  mobile-unit                 Details of associated mobile-units
  phrase-to-key               display the WEP keys generated by a passphrase
  qos-mapping                 Quality of Service mappings used for mapping
                              WMM access categories and 802.1p / DSCP tags
  radio                       Radio related commands
  regulatory                  Regulatory (allowed channel/power) information
                              for a particular country
  self-heal-config            Self-Healing Configuration Parameters
  sensor                      Wireless Intrusion Protection System parameters
  unapproved-aps              Unapproved APs seen by access-port or
                              mobile-unit scans
  wireless-switch-statistics  wireless-switch  statistics
  wlan                        Wireless LAN related parameters
RFS7000(config-if)#

RFS7000(config-if)#show wireless config
country-code            : None
adoption-pref-id        : 1
proxy-arp               : enabled
adopt-unconf-radio      : enabled
dot11-shared-key-auth   : disabled
ap-detection            : disabled
oversized-frames        : disabled
manual-wlan-mapping     : disabled
dhcp sniff state        : disabled
dhcp fix windows        : disabled
broadcast-tx-speed      : optimize-for-throughput
smart-scan 11a channels :
smart-scan 11bg channels:
RFS7000(config-if)#

RFS7000(config-if)#show spanning-tree mst
% Bridge up - Spanning Tree Enabled
% CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000000000000
% 1: CIST Reg Root Id 8000000000000000
% 1: CST Bridge Id 8000000000000000
% portfast bpdu-filter enabled
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 300 sec
% cisco interoperability not configured - Current cisco interoperability off
%
%   Instance        VLAN
%   0:              1-4095
RFS7000(config-if)#
```

7.1.15 shutdown

▶ *Interface Config commands*

Use this command to shutdown the selected interface.

Syntax

```
shutdown
```

Parameters

None.

Example

```
RFS7000(config-if)#shutdown
RFS7000(config-if)#
```

7.1.16 spanning-tree

▶ *Interface Config commands*

Use this command to configure spanning tree parameters.

Syntax

```
spanning-tree [bpdufilter(enable|disable)|bpduguard
(enable|disable)|edgeport|force-version <0-3>|guard (root)|link-type (point-to-
point|shared)|mst(<0-15>|port-cisco-interoperability)|portfast]

spanning-tree mst [<0-15>(cost <1-200000000>|port-priority <0-240>)|
port-cisco-interoperability (disable|enable)]
```

Parameters

bpdufilter (disable|enable)	Use this command to set a portfast BPDU filter for the port. Use the no parameter with this command to revert the port BPDU filter value to default. The spanning tree protocol sends BPDUs from all ports. Enabling the BPDU filter ensures PortFastenabled ports do not transmit or receive BPDUs.
bpduguard (disable|enable)	Use this command to enable or disable the BPDU guard feature on a port. Use the no parameter with this command to set the BPDU guard feature on a port to default values. When BPDU guard is set for a bridge, all portfast-enabled ports that have bpdu-guard set to default shut down the port upon receiving a BPDU. In this occurs, the BPDU is not processed. The port can be brought back either manually (using the no shutdown command), or by configuring the errdisable-timeout to enable the port after the specified interval.
edgeport	Enables an interface as an edgeport.
force-version <0-3>	Specifies the spanning-tree force version. A version identifier of less than 2 enforces the spanning tree protocol. Select from the following versions: • 0 – STP • 1 – Not supported. • 2 – RSTP • 3 – MSTP The default value for forcing the version is MSTP.
guard (root)	Enables the Root Guard feature for the port. The root guard disables the reception of superior BPDUs. The Root Guard ensures the port on which it is enabled is a designated port. If the Root Guard enabled port receives a superior BPDU, it goes to a discarding state. Use the no parameter with this command to disable the root guard feature.
link-type (point-to-point|shared)	Enables or disables point-to-point or shared link types. • point-to-point – enables rapid transition. • shared – disables rapid transition.

mst [<0-15> (cost <1-200000000>| port-priority <0-240>)| port-cisco-interoperability (disable|enable)]	Configures mst on a spanning tree. • <0-15> – Instance ID. • cost <1-200000000> – Path cost for a port. • port-priority <0-240> – Port priority for a bridge. • port-cisco-interoperability (disable|enable) – Enables or disables interoperability with Cisco's version of MSTP (which is incompatible with standard MSTP). • enable – Enables CISCO Interoperability. • disable – Disables CISCO Interoperability. The default value for is `disabled`.
portfast	Enables rapid transitions.

Example

```
RFS7000(config-if)#spanning-tree edgeport
RFS7000(config-if)#

RFS7000(config-if)#spanning-tree guard root
RFS7000(config-if)#

RFS7000(config-if)#spanning-tree link-type point-to-point
RFS7000(config-if)#

RFS7000(config-if)#spanning-tree link-type shared
RFS7000(config-if)#
```

7.1.17 speed

▸ *Interface Config commands*

Use this command to configure the speed of the selected interface in Mbps.

Syntax

```
speed(10|100|1000|auto)
```

Parameters

10	Forces 10 Mbps operation.
100	Forces 100 Mbps operation.
1000	Forces 1000 Mbps operation.
auto	Enables AUTO speed configuration.

Usage Guidelines

Set the interface speed to `auto` to detect and use the fastest speed avaiable. The speed detection is based on the connected network hardware.

Example

```
RFS7000(config-if)#speed auto
RFS7000(config-if)#

RFS7000(config-if)#speed 1000
RFS7000(config-if)#

RFS7000(config-if)#show interfaces ge2
Interface ge2
  Hardware Type Ethernet, Interface Mode Layer 2, address is 00-15-70-37-fb-73
  index=2002, metric=1, mtu=1500, (HAL-IF)  <UP,BROADCAST,MULTICAST>
  Speed: Admin 1G, Operational Unknown, Maximum 1G
  Duplex: Admin Auto, Operational Unknown
  Active Medium: Unknown
  Switchport Settings: Mode: Access, Access Vlan: 1
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 767, bytes 144486, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
RFS7000(config-if)#
```

7.1.18 static-channel-group

▶ *Interface Config commands*

Use this command to to add an interface to a static channel group.

Syntax

```
static-channel-group <1-4>
```

Parameters

<1-4>	Static channel group to associate the link with.

Usage Guidelines

This command aggregates individual giga port's into a single aggregate link to provide a larger bandwidth. Static channel group is used to provide additional bandwidth in multiples of 1Gbps on the switch. All MAC layer and higher protocols see only the static channel group (aggregate link) rather than the individual ports that comprise it.

Example

```
RFS7000(config-if)#static-channel-group 2
RFS7000(config-if)#
```

7.1.19 switchport

▶ *Interface Config commands*

Use this command to set switching mode characteristics for the selected interface. The mode can be either access or trunk.

> **NOTE** The ge interface earlier configured as a trunk with *all* VLAN's allowed on it looses its confiugration and has only VLAN 1 set to allowed.

Syntax

```
switchport(access|mode|trunk)
switchport access vlan <1-4094>
switchport mode(access|trunk)
switchport trunk(allowed|native)
switchport trunk allowed vlan(add|none|remove)<VLAN_ID>
switchport trunk native(tagged|vlan<1-4094>)
```

Parameters

access (vlan) <1-4094>	Sets access mode characteristics. • vlan <1-4094> – Sets the VLAN when an interface is in access mode.
mode (access|trunk)	Sets the mode of the Layer2 interface. • access – Sets the Layer2 interface as access. • trunk – Sets the Layer2 interface as trunk.
trunk (allowed|native)	Sets trunking mode characteristics. • allowed – Sets trunking mode allowed VLAN characteristics. • native – Sets native trunking characteristics.
trunk allowed (vlan) (add|none|remove) <VLAN_ID>	Sets trunking mode allowed VLAN characteristics. • vlan – Sets the allowed VLANs. • add – Adds a VLANs to the current list. • none – Restricts VLANs to Xmit/Rx through the Layer2 interface. • remove – Removes VLANs from the current list. • VLAN_ID – The list of the VLAN IDs to be added/removed. For example, 10-20,25,30-35.
trunk native (tagged | vlan <1-4094>)	Sets native trunking characteristics. • tagged – Sets the native VLAN for classifying untagged traffic. • vlan <1-4094> – Sets the native VLAN for classifying untagged traffic when the interface is in trunking mode.

Usage Guidelines

The interface ge1-ge4 can be configured either as trunk or in access mode. Interface when configured as trunk allows packets from the given list of VLANS that is added to the trunk. Inerface when configured as access will allow packets only from the native VLANs.

Example

```
RFS7000(config-if)#switchport mode access
RFS7000(config-if)#
```

7.1.20 tunnel

▶ *Interface Config commands*

Use this command to configure protocol-over-protocol tunneling.

Syntax

```
tunnel(destination|source|ttl)
tunnel destination A.B.C.D
tunnel source A.B.C.D
tunnel ttl<1-255>
```

Parameters

destination	Destination of tunnel packets.
source	Source of tunnel packets.
A.B.C.D	Internet Protocol (IP).
ttl	Sets the time to live interval.
<1-255>	The time to live (ttl) in seconds.

Example

```
RFS7000(config)#interface tunnel 1

RFS7000(config-if)#tunnel destination 172.168.200.20

RFS7000(config-if)#tunnel ttl 33

RFS7000(config)#show interfaces tunnel 1
Interface tunnel1
  Hardware Type Tunnel, Interface Mode Layer 3
  index=13, metric=1, mtu=1476, (PAL-IF)  <UP,POINTOPOINT,RUNNING,NOARP>
  Tunnel source 172.168.100.20, destination 172.168.200.20
  Tunnel protocol/transport GRE/IP,  Tunnel TTL 33
    input packets 0, bytes 0, dropped 0, multicast packets 0
    input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
    output packets 0, bytes 0, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
RFS7000(config)#
```

spanning tree-mst Instance

Use the **`(config-mst)`** instance to configure the *Multi Spanning Tree Protocol* (MSTP). Use `(config)#spanning-tree mst configuration` to reach this instance.

8.1 mst Config commands

Table 8.1 summarizes the **`config-mst`** commands.

Table 8.1 MSTP Config Command Summary

Command	***Description***	***Ref.***
clrscr	Clears the display screen.	page 8-2
end	Ends the current mode and moves to the EXEC mode.	page 8-3
exit	Ends the current mode and moves to the previous mode.	page 8-4
help	Describes the interactive help system.	page 8-5
instance	Assigns a VLAN to the bridge instance.	page 8-6
name	Sets a name for the MST region.	page 8-7
no	Negates a command or sets defaults.	page 8-8
revision	Configures the revision number of the MST bridge.	page 8-9
service	Service commands.	page 8-10
show	Shows running system information.	page 8-12

8.1.1 clrscr

▸ *mst Config commands*

Use this command to clear the display.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-mst)#clrscr
RFS7000(config-mst)#
```

8.1.2 end

▶ *mst Config commands*

Use this command to end and exit from the current mode and move to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-mst)#end
RFS7000#
```

8.1.3 exit

▶ *mst Config commands*

Use this command to end the current mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-mst)#exit
RFS7000(config)#
```

8.1.4 help

mst Config commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-mst)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-mst)#
```

8.1.5 instance

▶ mst Config commands

Use this command to associate VLAN(s) with an instance.

Syntax

```
instance <1-15> vlan <VLAN_ID>
```

Parameters

<1-15>	Enters the instance ID to which the VLAN is associated.
vlan <VLAN_ID>	Enters the VLAN ID for its association with an instance.

Usage Guidelines

MSTP works based on instances. An instance is agroup of VLAN's with a common spanning tree. A single VLAN caanot be associated with multiple instances.

Switches with same instance - VLAN mapping, revision number and region names creates a region. Switches in the same region exchange *bridge protocol data units* (BPDU) with instance record information in it.

Example

The example below creates an instance named 10 and maps VLAN 20 to it.

```
RFS7000(config-mst)#instance 10 vlan 20
RFS7000(config-mst)#
```

8.1.6 name

▶ *mst Config commands*

Use this command to set a name for the MST region.

Syntax

```
name (region name)
```

Parameters

region name	MST region name.

Example

```
RFS7000(config-mst)#name MyRegion
RFS7000(config-mst)#
```

8.1.7 no

▶ *mst Config commands*

Use this command to negate a command or set defaults.

Syntax

```
no [instance|name|revision]
```

Parameters

instance	Instance.
name	MST region.
revision	Revision number for configuration information.

Usage Guidelines

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFS7000(config-mst)#no instance 10 vlan 20
RFS7000(config-mst)#

RFS7000(config-mst)#no name MyRegion
RFS7000(config-mst)#

RFS7000(config-mst)#no revision
RFS7000(config-mst)#
```

8.1.8 revision

▶ *mst Config commands*

Use this command to configure the revision number of the MST bridge.

Syntax

```
revision <0-255>
```

Parameters

0-255	Revision number for configuration information.

Example

```
RFS7000(config-mst)#revision 20
RFS7000(config-mst)#
```

8.1.9 service

▶ *mst Config commands*

Use this command to invoke the service commands needed to trobuleshoot or debug `(config-if)` instance configurations.

Syntax

```
service(show) (cli)
```

Parameters

show (cli)	Shows running system information. • *cli* – Show CLI tree of current mode.

Example

```
RFS7000(config-mst)*#service show cli
MSTI configuration mode:
+-bridge
  +-instance
    +-<1-15> [bridge instance <1-15>]
      +-vlan
        +-<1-4094> [bridge instance <1-15> vlan <1-4094>]
  +-region
    +-REGION_NAME [bridge region REGION_NAME]
  +-revision
    +-REVISION_NUM [bridge revision REVISION_NUM]
+-clrscr [clrscr]
+-end [end]
+-exit [exit]
+-help [help]
+-no
  +-bridge
    +-instance
      +-<1-15> [no bridge instance <1-15>]
        +-vlan
          +-<1-4094> [no bridge instance <1-15> vlan <1-4094>]
    +-region [no bridge region]
    +-revision [no bridge revision]
+-quit [quit]
+-s
  +-commands [show commands]
    +-WORD [show commands WORD]
  +-running-config [show running-config]
    +-full [show running-config full]
    +-include-factory [show running-config include-factory]
+-service
  +-show
    +-cli [service show cli]
+-show
  +-access-list [show access-list]
    +-<1-99> [show access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)]
    +-<100-199> [show access-list (<1-99>|<100-199>|<1300-1999>|<2000-
2699>|WORD)]
    +-<1300-1999> [show access-list (<1-99>|<100-199>|<1300-1999>|<2000-
2699>|WORD)]
    +-<2000-2699> [show access-list (<1-99>|<100-199>|<1300-1999>|<2000-
2699>|WORD)]
    +-WORD [show access-list (<1-99>|<100-199>|<1300-1999>|<2000-2699>|WORD)]
  +-aclstats
..........................................................................
.................................................................................
.................................................................................
```

```
.................................................................................................
.................................................................................................
.................................................................................................
.......................
RFS7000(config-mst)#
```

8.1.10 show

▶ *mst Config commands*

Use this command to view current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Example

```
RFS7000(config-mst)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                Encryption related commands
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   MAC access-list assignment
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         spanning-tree Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl

RFS7000(config-mst)#show
```

```
RFS7000(config-mst)#show access-list
Extended IP access list 110
    permit ip 192.168.1.0/24 192.168.100.0/24 rule-precedence 5
    permit ip 192.168.63.0/24 192.168.100.0/24 rule-precedence 63
    permit ip 192.168.157.0/24 192.168.100.0/24 rule-precedence 157
RFS7000(config-mst)#

RFS7000(config-mst)#show wlan-acl all
WLAN port: 102
  Inbound IP Access List : 110
  Inbound MAC Access List :

  Outbound IP Access List:
  Outbound MAC Access List :
RFS7000(config-mst)#
```

8.2 Configuring Interface using MSTP

MSTP runs by default. All VLANs are in default instance 0 by default.

1. Use the following command to create a non-default instance and region configuration using the `mst config` mode.

   ```
   RFS7000(config-mst)#instance 1 vlan <vlan-id>
   ```

2. Use the following to enable/disable MSTP.

   ```
   RFS7000(config)#bridge multiple-spanning-tree
   ```

3. Use the following command to configure spanning-tree.

   ```
   RFS7000(config)#bridge multiple-spanning-tree
   RFS7000(config)#spanning-tree
   ```

4. Use the following command to configure spanning-tree for ports.

   ```
   RFS7000(config-if)#spanning-tree
   ```

Extended ACL Instance

Use the **(config-ext-nacl)** instance to configure **ip access-list extended** ACLs..

9.1 Extended ACL Config Commands

Table 9.1 summarizes the **config-ext-nacl** commands.

Table 9.1 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen.	page 9-2
deny	Specifies packets to reject.	page 9-3
end	Ends the current mode and changes to the EXEC mode.	page 9-7
exit	Ends the current mode and moves back to the previous mode.	page 9-8
help	The interactive help system.	page 9-9
mark	Specifies packets to mark.	page 9-10
no	Negates a command or set default values.	page 9-14
permit	Specifies packets to forward.	page 9-15
service	Service commands.	page 9-19
show	Shows running system information.	page 9-20
terminal	Sets terminal line parameters.	page 9-22

9.1.1 clrscr

▶ *Extended ACL Config Commands*

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-ext-nacl)#clrscr
RFS7000(config-ext-nacl)#
```

9.1.2 deny

▶ *Extended ACL Config Commands*

Use this command to specify packets to reject.

Syntax

```
deny(icmp|ip|tcp|udp)

deny {ip} {source/source-mask | host source | any} {destination/destination-mask
| host destination | any} [log] [rule-precedence access-list-entry precedence]

deny {icmp} {source/source-mask | host source | any} {destination/ destination-
mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-
precedence access-list-entry precedence]

deny {tcp|udp} {source/source-mask | host source | any} [operator source-port]
{destination/destination-mask | host destination | any} [operator destination-
port] [log] [rule-precedence access-list-entry precedence]
```

Parameters

deny {**ip**} {source/source-mask | host source | any} {destination/destination-mask | host destination | any} [log] [rule-precedence access-list-entry precedence]	Use with a **deny** command to reject IP packets. • deny – Action type on an ACL. • {**ip**} – Specifies IP ((to match any protocol). • {source/source-mask | host source | any} – The keyword **source** is the source IP address of the network or host in dotted decimal format. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0. • **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32. • {destination/destination-mask | host destination | any} – The destination host IP address or destination network address. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

deny {**icmp**} {source/ source-mask | host source | any} {destination/ destination-mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-precedence access-list-entry precedence]	Use with **deny** command to reject icmp packets. • deny – Action types on an ACL. • {**icmp**} – Specifies icmp as the protocol. • {source/source-mask | host source | any} – **source** is the source IP address of the network or host in dotted decimal format. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0. • **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32. • {destination/ destination-mask | host destination | any} – The destination host IP address or destination network address. • [icmp-type |icmp-type icmp-code] – **ICMP type** value from 0 to 255. Valid only for protocol type icmp. **ICMP code** value from 0 to 255. Valid only for protocol type icmp. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

deny {**tcp|udp**} {source/ source-mask | host source | any} [operator source-port] {destination/ destination-mask | host destination | any} [operator destination-port] [log] [rule-precedence access-list-entry precedence]	Use with **deny** command to reject tcp or udp packets. • deny – Action types on an ACL. • {**tcp|udp**} – Specify tcp or udp as protocol. • {source/source-mask | host source | any} – The keyword **source** is the source IP address of the network or host in dotted decimal format. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0. • **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32. • [operator source-port] – Valid only for tcp or udp protocols. Valid values are **eq** and **range**. • range – Specifies the protocol range (starting and ending protocol numbers). • port – Valid Port number. • {destination/destination-mask | host destination | any} – The destination host IP address or destination network address. • [operator destination-port] – Specifies the destination port. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Use this command to deny traffic between network's/host's based on the protocol type selected in the access list configuration. The following protocol types are supported:

- ip
- icmp
- tcp
- udp

The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against the ACE's in the ACL. It is allowed/denied based on the ACL configuration.

- Filtering on protocol types tcp/udp allows the user to specify port numbers as filtering criteria.

- Select the protocol type icmp to allow/deny icmp packets. Selecting icmp provies the option of filtering icmp packets based on icmp type and code.

NOTE The log option is functional only for router ACL's. The log option causes an informational logging message about the packet that matches the entry to be sent to the console.

Example

The following example denies traffic between two subnets.

```
RFS7000(config-ext-nacl)#deny ip 192.168.2.0/24 192.168.1.0/24
RFS7000(config-ext-nacl)#permit ip any any
RFS7000(config-ext-nacl)#
```

The following example denies tcp traffic with source port range between 20 - 23 from the source subnet to destination sub net.

```
RFS7000(config-ext-nacl)#deny tcp 192.168.1.0/24 192.168.2.0/24 range 20 23
RFS7000(config-ext-nacl)#permit ip any any
RFS7000(config-ext-nacl)#
```

The following example denies udp traffic with source port range between 20 - 23 from the source subnet to destination sub net.

```
RFS7000(config-ext-nacl)#deny udp 192.168.1.0/24 192.168.2.0/24 range 20 23
RFS7000(config-ext-nacl)#permit ip any any
RFS7000(config-ext-nacl)#
```

The following example denies icmp traffic any source to any destination. The keyword *any* is used to match any source or destination IP address.

```
RFS7000(config-ext-nacl)#deny icmp any any
RFS7000(config-ext-nacl)#permit ip any any
RFS7000(config-ext-nacl)#
```

9.1.3 end

▶ *Extended ACL Config Commands*

Use this command to end and exit from the current mode and change to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-ext-nacl)#end
RFS7000#
```

9.1.4 exit

▶ *Extended ACL Config Commands*

Use this command to end current mode and go to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-ext-nacl)#exit
RFS7000(config)#
```

9.1.5 help

Extended ACL Config Commands

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-ext-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-ext-nacl)#
```

9.1.6 mark

▶ *Extended ACL Config Commands*

Use this command to mark specific packets.

Syntax

```
mark {dot1p <0-7> | tos <0-255>}} {ip} {source/source-mask | host source | any}
{destination/destination-mask  | host destination | any} [log] [rule-precedence
access-list-entry precedence]

mark {dot1p <0-7> | tos <0-255>}} {icmp} {source/source-mask | host source | any}
{destination/ destination-mask | host destination | any} [icmp-type | [icmp-type
icmp-code]] [log] [rule-precedence access-list-entry precedence]

mark {dot1p <0-7> | tos <0-255>}} {tcp|udp} {source/source-mask | host source |
any} [operator source-port] {destination/destination-mask | host destination |
any} [operator destination-port] [log] [rule-precedence access-list-entry
precedence]
```

Parameters

mark {dot1p <0-7> | tos <0-255>}} {**ip**} {source/ source-mask | host source | any} {destination/ destination-mask | host destination | any} [log] [rule-precedence access-list-entry precedence]	Use with the **mark** command to specify IP packets as marked. • mark {dot1p <0-7> | tos <0-255>} – Action types on an ACL. The action type `mark` is functional only over a Port ACL. • dot1p <0-7> – Used only with action type `mark` to specify 8021p priority values. • tos <0-255> – Used only with action type `mark` to specify Type Of Service (tos) values. • {**ip**} – Specify IP (to match any protocol). • {source/source-mask | host source | any} – The keyword **source** is the source IP address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0. • **host** is an abbreviation for the exact source (A.B.C.D) and source-mask bits equal to 32. • {destination/destination-mask | host destination | any} – The destination host IP address or destination network address. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

<table>
<tr>
<td>mark {dot1p <0-7&gt; | tos <0-255&gt;}} {<b>icmp</b>} {source/source-mask | host source | any} {destination/ destination-mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-precedence access-list-entry precedence]</td>
<td>Use with the <b><code>mark</code></b> command to specify icmp packets as marked.
• mark {dot1p <0-7&gt; | tos <0-255>} – Action types on an ACL. The action type <code>mark</code> is functional only over a Port ACL.
• {<b>icmp</b>} – Specify icmp as protocol.
• {source/source-mask | host source | any} – <b>source</b> is the source IP address of the network or host in dotted decimal format. Source-mask is the network mask. For example, 10.1.1.10/24 indicates that the first 24 bits of the source IP are used for matching.
  • <b>any</b> is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0.
  • <b>host</b> is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32.
• {destination/ destination-mask | host destination | any} – The destination host IP address or destination network address.
• [icmp-type |icmp-type icmp-code] – <b>ICMP type</b> value from 0 to 255. Valid only for protocol type icmp. <b>ICMP code</b> value from 0 to 255. Valid only for protocol type icmp.
• [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs.
• [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.</td>
</tr>
</table>

mark {dot1p <0-7> | tos <0-255>}} {**tcp|udp**} {source/source-mask | host source | any} [operator source-port] {destination/destination-mask | host destination | any} [operator destination-port] [log] [rule-precedence access-list-entry precedence]	Use with the **`mark`** command to specify tcp or udp packets as marked. • mark {dot1p <0-7> | tos <0-255>} – Action types on an ACL. The action type `mark` is functional only over a Port ACL. • {**tcp|udp**} – Specifies tcp or udp as the protocol used. • {source/source-mask | host source | any} – **source** is the source IP address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates that the first 24 bits of the source IP are used for matching. • **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0. • **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32. • [operator source-port] – Valid only for tcp or udp protocols. Valid values are **eq** and **range**. • range – Specifies the protocol range (starting and ending protocol numbers). • port – Valid port number. • {destination/destination-mask | host destination | any} – The destination host IP address or destination network address. • [operator destination-port] – Specifies the destination port. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

This command marks traffic between network's/host's based on the protocol type selected in the access list configuration.

Use mark option to specify the t*ype of service* (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

The following types of protocols are supported:

- ip
- icmp
- tcp
- udp

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is marked based on the ACL configuration.

- Filtering on Protocol types tcp/udp allows the user to specify port numbers as filtering criteria.

- Select the protocol type icmp to allow/deny icmp packets. Selecting icmp protocol allow you the option of filtering icmp packets based on icmp type and icmp code.

✓ **NOTE** The log option is functional only for router ACL's. The log option provides an informational logging message about the packet matching the entry sent to the console.

Example

The example below marks the dot1p priority value in the ethernet header to 5 to all tcp traffic coming from the source subnet.

```
RFS7000(config-ext-nacl)#mark 8021p 5 tcp 192.168.2.0/24 any
RFS7000(config-ext-nacl)#
```

The example below marks the tos value in the IP header to 245 to all tcp traffic coming from the source subnet.

```
RFS7000(config-ext-nacl)#mark tos 245 tcp 192.168.2.0/24 any
RFS7000(config-ext-nacl)#
```

9.1.7 no

▶ *Extended ACL Config Commands*

Use this command to negate a command or set its defaults.

Syntax

```
no(deny|mark|permit)
```

This command negates all the syntax combinations used in *deny*, *mark* and *permit* commands to configure the Extended ACL.

Parameters

deny	Specifies packets to reject.
mark	Specifies packets to mark.
permit	Specifies packets to forward.

Usage Guidelines

Use the no command to remove an access list control entry. Provide the rule-precedence value when using the no command.

Example

```
RFS7000(config-ext-nacl)#no mark 8021p 5 tcp 192.168.2.0/24 any rule-precedence 
10
RFS7000(config-ext-nacl)#

RFS7000(config-ext-nacl)#no permit ip any any rule-precedence 10
RFS7000(config-ext-nacl)#

RFS7000(config-ext-nacl)#no deny icmp any any rule-precedence 10
RFS7000(config-ext-nacl)#
```

9.1.8 permit

▶ *Extended ACL Config Commands*

Use this command to permit specific packets.

NOTE ACLs do not allow DHCP messages to flow through by default. Configure an Access Control Entry (ACE) to allow DHCP messages to flow through.

```
RFS7000(config-ext-nacl)#permit ip 192.168.1.0/24 192.168.2.0/24
RFS7000(config-ext-nacl)#permit ip any host 255.255.255.255
RFS7000(config-ext-nacl)#
```

Syntax

```
permit {ip} {source/source-mask | host source | any} {destination/destination-
mask  | host destination | any} [log] [rule-precedence access-list-entry
precedence]

permit {icmp} {source/source-mask | host source | any} {destination/ destination-
mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-
precedence access-list-entry precedence]

permit{tcp|udp} {source/source-mask | host source | any} [operator source-port]
{destination/destination-mask | host destination | any} [operator destination-
port] [log] [rule-precedence access-list-entry precedence]
```

Parameters

permit {**ip**}
{source/source-mask | host source | any}
{destination/destination-mask | host destination | any}
[log]
[rule-precedence access-list-entry precedence]
	Use the **permit** command to allow **IP** packets.
	• permit – Action types on an ACL.
	• {**ip**} – Specify IP (to match any protocol).
	• {source/source-mask | host source | any} – **source** is the source IP address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching.
	  • **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0.
	  • **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32.
	• {destination/destination-mask | host destination | any} – The destination host IP address or destination network address.
	• [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs.
	• [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

permit {**icmp**} {source/source-mask | host source | any} {destination/ destination-mask | host destination | any} [icmp-type | [icmp-type icmp-code]] [log] [rule-precedence access-list-entry precedence]	Use with the **`permit`** command to allow **icmp** packets. • permit – Action types on an ACL. • {**icmp**} – Specifies icmp as the protocol. • {source/source-mask | host source | any} – The keyword **source** is the source IP address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0. • **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32. • {destination/ destination-mask | host destination | any} – The destination host IP address or destination network address. • [icmp-type |icmp-type icmp-code] – **ICMP type** value from 0 to 255. Valid only for protocol type icmp. **ICMP code** value from 0 to 255. Valid only for protocol type icmp. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

permit{**tcp|udp**} {source/source-mask | host source | any} [operator source-port] {destination/destination-mask | host destination | any} [operator destination-port] [log] [rule-precedence access-list-entry precedence]	Use with the **`permit`** command to allow **tcp or udp** packets. • permit – Action types on an ACL. • {**tcp|udp**} – Specify tcp or udp as protocol. • {source/source-mask | host source | any} – **source** is the source IP address of the network or host in dotted decimal. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching. • **any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0. • **host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32. • [operator source-port] – Valid only for tcp or udp protocols. Valid values are **eq** and **range**. • range – Specify the protocol range (starting and ending protocol numbers). • port – Valid Port number. • {destination/destination-mask | host destination | any} – The destination host IP address or destination network address. • [operator destination-port] – Specify the destination port. • [log] – Generates log messages when the packet coming from the interface matches the ACL entry. Log messages are generated only for router ACLs. • [rule-precedence access-list-entry precedence] – Integer value between 1-5000. This value sets the rule precedence in the ACL.

Usage Guidelines

Use this command to permit traffic between network's/host's based on the protocol type selected in the access list configuration. The following types of protocols are supported:

- ip
- icmp
- tcp
- udp

The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed based on the ACL configuration.

- Filtering on Protocol types tcp/udp allows the user to specify port numbers as filtering criteria.

- Select the protocol type icmp to allow/deny icmp packets. Selecting icmp protocol allow you the option of filtering icmp packets based on icmp type and icmp code.

✓ **NOTE** The log option is functional only for router ACL's. The log option causes an informational logging message about the packet matching the entry sent to the console.

Example

The example below allows IP traffic from the source subnet to destination subnet and denies all other traffic over an interface.

```
RFS7000(config-ext-nacl)#permit ip 192.168.1.10/24 192.168.2.0/24 rule-precedence
40
RFS7000(config-ext-nacl)#
```

The example below permits telnet from the source subnet and the destination subnet and denies all other traffic over an interface.

```
RFS7000(config-ext-nacl)#permit tcp 192.168.4.0/24 192.168.5.0/24 eq 23 rule-pre
cedence 10
RFS7000(config-ext-nacl)#
```

The example below permits icmp based traffic and denies all other traffic over an interface.

```
RFS7000(config-ext-nacl)#permit icmp any any rule-precedence 30
RFS7000(config-ext-nacl)#)#
```

9.1.9 service

▶ *Extended ACL Config Commands*

Use this command to invoke service commands to troubleshoot or debug **(config-if)** instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell)
```

Parameters

clear	Removes specified support information.
diag-shell	Provides diagnostic shell access to debug and test the RFS7000 Switch.
save-cli	Saves the CLI tree for all modes in html format.
show	Shows running system information.
start-shell	Provides shell access.

Example

```
RFS7000(config-ext-nacl)#service diag-shell

Diagnostic shell started for testing
diag >
  boot            Reboots the switch
  delete          Deletes specified file from the system.
  exit            Exit from the CLI
  fallback        Configures firmware fallback feature
  help            Description of the interactive help system
  logout          Exit from the CLI
  no              Negate a command or set its defaults
  reload          Halt and perform a warm reboot
  service         Service Commands
  show            Show running system information
  upgrade         Upgrade firmware image

RFS7000(config-ext-nacl)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
RFS7000(config-ext-nacl)#

RFS7000(config-ext-nacl)#service show ?
  cli              Show CLI tree of current mode
  command-history  Display command (except show commands) history.
  crash-info       Display information about core, panic and AP dump files
  info             Show snapshot of available support information
  last-passwd      Display last password used to enter shell
  reboot-history   Show reboot history
  startup-log      Show startup log
  upgrade-history  Show upgrade history

RFS7000(config-ext-nacl)#service show

RFS7000(config-ext-nacl)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:
```

9.1.10 show

▶ Extended ACL Config Commands

Use this command to view the current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays all the parameters for which the information can be viewed using the show command.

Usage Guidelines

The `show access-list` command displays all the access lists configured in the switch in the console. Mention the access list name or number to view the details of a particular ACL.

Example

```
RFS7000(config-ext-nacl)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

RFS7000(config-ext-nacl)#show
```

```
RFS7000(config-ext-nacl)#show access-list
Extended IP access list 101
    deny ip 192.168.1.0/24 192.168.2.0/24 rule-precedence 10
    permit ip any any rule-precedence 20
Extended IP access list 110
    deny ip host 192.168.1.95 host 192.168.2.98 log rule-precedence 10
    permit ip any any rule-precedence 20
Extended IP access list symbol
    deny tcp 192.168.2.0/24 192.168.1.0/24 rule-precedence 10
    permit ip any any rule-precedence 20
RFS7000(config-ext-nacl)#
```

9.1.11 terminal

▶ Extended ACL Config Commands

Use this command to set the length /number of lines displayed on the terminal window.

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copies debug output to the current terminal line.
no	Negates a command or set its defaults. • monitor – Copies debug output to the current terminal line.

Usage Guidelines

By default, the log messages are generally not displays over a telnet session. Use the `terminal monitor` command to view the log messages over a telnet session.

Example

```
RFS7000(config-ext-nacl)#terminal monitor
RFS7000(config-ext-nacl)#

RFS7000(config-ext-nacl)#terminal no monitor
RFS7000(config-ext-nacl)#
```

10

Standard ACL Instance

Use the **`(config-std-nacl)`** instance to configure **`ip access-list standard`** ACLs. Standard ACLs allow filtering based on the source address only.

10.1 Standard ACL Config Commands

Table 10.1 summarizes **`config-std-nacl`** commands.

Table 10.1 Extended ACL Config Command Summary

Command	***Description***	***Ref.***
clrscr	Clears the display screen.	page 10-2
deny	Specifies packets to reject.	page 10-3
end	Ends the current mode and change to EXEC mode.	page 10-4
exit	Ends the current mode and moved back to the previous mode.	page 10-5
help	The interactive help system.	page 10-6
mark	Specifies packets to mark.	page 10-7
no	Negates a command or set its defaults.	page 10-8
permit	Specifies packets to forward.	page 10-9
service	Service commands.	page 10-10
show	Shows the running system information.	page 10-11
terminal	Sets terminal line parameters.	page 10-13

10.1.1 clrscr

▶ *Standard ACL Config Commands*

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-std-nacl)#clrscr
RFS7000(config-std-nacl)#
```

10.1.2 deny

▶ *Standard ACL Config Commands*

Use this command to specify packets to reject.

Syntax

```
deny(A.B.C.D/M|any|host)
deny any(log|rule-precedence)
deny any log(rule-precedence)<1-5000>
deny any rule-precedence<1-5000>
deny host A.B.C.D
```

Parameters

A.B.C.D/M	Source IP address range to match.
any	Any source IP address. • log – Log matches against this entry. • rule-precedence *<1-5000>* – Access-list entry precedence.
host	Single host address. • A.B.C.D – Exact source IP address to match.

Usage Guidelines

Use this command to deny traffic based on source IP address or network address. The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed/denied based on the ACL configuration.

☑ **NOTE** The log option is functional only for router ACL's. The log option results in an informational logging message for the packet matching the entry sent to the console.

Example

The example below denies all traffic entering the interface. A log message is generated in the console whenever the interface receives a packet.

```
RFS7000(config-std-nacl)#deny any log rule-precedence 50
RFS7000(config-std-nacl)#
```

The example below denies traffic from the source network (xxx.xxx.1.0/24) and allows all other traffic to flow through the interface.

```
RFS7000(config-std-nacl)#deny xxx.xxx.1.0/24 rule-precedence 60
RFS7000(config-std-nacl)#permit any
```

10.1.3 end

▸ *Standard ACL Config Commands*

Use this command to exit the current mode and move to the PRIV EXEC mode. The prompt changes to **RFS7000#**.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-std-nacl)#end
RFS7000#
```

10.1.4 exit

▸ *Standard ACL Config Commands*

Use this command to end the current mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to **RFS7000(config)#**.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-std-nacl)#exit
RFS7000(config)#
```

10.1.5 help

▶ *Standard ACL Config Commands*

Use this command to access the system’s interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-std-nacl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-std-nacl)#
```

10.1.6 mark

▶ *Standard ACL Config Commands*

Use this command to mark specific packets.

Syntax

```
mark(8021.1p<0-7>|tos<0-255>)(A.B.C.D/M|any|host)

mark(8021.1p<0-7>|tos<0-255>)any|host(log|rule-precedence<1-5000>|
|A.B>C.D)
```

Parameters

8021.1p<*0-7*>|tos<*0-255*>)	• Specifies .1p priority value between 0 and 7 • Specifies a *Type of Service* (tos) value between 0 and 255.
(A.B.C.D/M|any|host)	**source** is the source IP address of the network or host in dotted decimal format. Source-mask is the network mask. For example, 10.1.1.10/24 indicates the first 24 bits of the source IP are used for matching.
any	**any** is an abbreviation for source IP of 0.0.0.0 and source-mask bits equal to 0.
host (log|rule-precedence<*1-5000*>||A.B>C.D)	**host** is an abbreviation for exact source (A.B.C.D) and source-mask bits equal to 32.

Usage Guidelines

UUse this command to mark traffic from the source network/host. Use the mark option to specify the t*ype of sservice* (tos) and priority value. The tos value is marked in the IP header. The 802.1p priority value is marked din the frame.

r When the interface receives the packet, its content is checked against the ACE's in the ACL. It is marked based oon the ACL configuration.

☑ **NOTE** The log option is functional only for router ACL's. The log option results in an informational logging message about the packet matching the entry sent to the console.

Example

TThe example below marks the *type of service* (tos) value to 254 for all traffic coming from the source network.

```
RFS7000(config)#access-list 3 mark tos 254 xxx.xxx.3.0/24
 RFS7000(config)#access-list 3 permit any
```

10.1.7 no

▶ *Standard ACL Config Commands*

Use this command to negate a command or set its defaults.

Syntax

```
no(deny|mark|permit)
```

This command negates all the syntax combinations used in *deny*, *mark* and *permit* commands to configure the Extended ACL.

Parameters

deny	Specifies packets to reject.
mark	Specifies packets to mark.
permit	Specifies packets to forward.

Example

```
RFS7000(config-std-nacl)#no permit any rule-precedence 10
RFS7000(config-std-nacl)#

RFS7000(config-std-nacl)#no deny any rule-precedence 20
RFS7000(config-std-nacl)#

RFS7000(config-std-nacl)#no mark tos 4 192.168.2.0/24 rule-precedence 30
RFS7000(config-std-nacl)#
```

10.1.8 permit

▶ *Standard ACL Config Commands*

Use this command to permit specific packets.

Syntax

```
permit(A.B.C.D/M|any|host)
permit any(log|rule-precedence)
permit any log(rule-precedence)<1-5000>
permit any rule-precedence<1-5000>
permit host A.B.C.D
```

Parameters

A.B.C.D/M	Source IP address range to match.
any	Any source IP address. • log – Log matches against this entry. • rule-precedence<*1-500*> – Access-list entry precedence.
host	Single host address. • A.B.C.D – Exact source IP address to match.

Usage Guidelines

Use this command to allow traffic based on the source IP address or network address. The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed based on the ACL configuration.

✓ **NOTE** The log option is functional only for router ACL's. The log option causes an informational logging message about the packet matching the entry sent to the console.

Example

The example below permits all the traffic that comes to the interface.

```
RFS7000(config-std-nacl)#permit any rule-precedence 50
RFS7000(config-std-nacl)#
```

The example below permits traffic from the source network and provides a log message for the same.

```
RFS7000(config-std-nacl)#permit xxx.xxx.1.0/24 log rule-precedence 60
RFS7000(config-std-nacl)#
```

10.1.9 service

▶ *Standard ACL Config Commands*

Use this command to invoke service commands to troubleshoot or debug **`(config-if)`** instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Removes specified support information.
diag-shell	Provides diagnostic shell access to debug and test the switch.
save-cli	Saves the CLI tree for all modes in html format.
show	Shows running system information.
start-shell	Provides shell access.
tethereal	

Example

```
RFS7000(config-std-nacl)#service diag-shell
Diagnostic shell started for testing
diag >

RFS7000(config-std-nacl)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
RFS7000(config-std-nacl)#

RFS7000(config-std-nacl)#service show ?
  cli               Show CLI tree of current mode
  command-history   Display command (except show commands) history.
  crash-info        Display information about core, panic and AP dump files
  info              Show snapshot of available support information
  last-passwd       Display last password used to enter shell
  reboot-history    Show reboot history
  startup-log       Show startup log
  upgrade-history   Show upgrade history
RFS7000(config-std-nacl)#service show

RFS7000(config-std-nacl)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
Password:
RFS7000(config-std-nacl)#
```

10.1.10 show

▸ *Standard ACL Config Commands*

Use this command to view current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Usage Guidelines

`show access-list` command displays all the access lists configured in the switch in the console. Provide the access list name or number to view the details of a particular ACL.

Example

```
RFS7000(config-std-nacl)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

RFS7000(config-std-nacl)#show
```

```
RFS7000(config-std-nacl)#show access-list
Standard IP access list 1
    permit any rule-precedence 10
Extended IP access list 101
    deny ip 192.168.1.0/24 192.168.2.0/24 rule-precedence 10
    permit ip any any rule-precedence 20
Extended IP access list 110
    deny ip host 192.168.1.95 host 192.168.2.98 log rule-precedence 10
    permit ip any any rule-precedence 20
Standard IP access list moto
    deny 192.168.1.0/24 rule-precedence 10
    permit any rule-precedence 20
Extended IP access list symbol
    deny tcp 192.168.2.0/24 192.168.1.0/24 rule-precedence 10
    permit ip any any rule-precedence 20
RFS7000(config-std-nacl)#
```

10.1.11 terminal

▶ *Standard ACL Config Commands*

Use this command to set the length /number of lines displayed on the terminal.

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copies debug output to the current terminal line.
no	Negates a command or set its defaults. • monitor – Copies debug output to the current terminal line.

Usage Guidelines

By default, log messages are generally not displayed over a Telnet session. Use the `terminal monitor` command to view the log messages over a Telnet session.

Example

```
RFS7000(config-std-nacl)#terminal monitor
RFS7000(config-std-nacl)#

RFS7000(config-std-nacl)#terminal no monitor
RFS7000(config-std-nacl)#
```

Extended MAC ACL Instance

Use the **(config-ext-macl)** instance to configure **mac access-list extended** ACLs associated with the switch.

Use decimal value representation of ethertypes to implement permit/deny/mark packet. The command set for Extended MAC ACLs provides hexadecimal values for each of its listed ether types. The switch supports all ethertypes. Use the decimal equvilant of the ethertype listed in the CLI or for any other ethertype.

11.1 MAC Extended ACL Config Commands

Table 11.1 summarizes the **`config-ext-macl`** commands.

Table 11.1 Extended ACL Config Command Summary

Command	Description	Ref.
clrscr	Clears the display screen.	page 11-3
deny	Specifies packets to reject.	page 11-4
end	Ends the current mode and moves to the EXEC mode.	page 11-6
exit	Ends the current mode and moves to the previous mode.	page 11-7
help	Describes the interactive help system.	page 11-8
mark	Specifies packets to mark.	page 11-9
no	Negates a command or sets defaults.	page 11-11
permit	Specifies packets to forward.	page 11-12
service	Service commands.	page 11-14
show	Shows running system information.	page 11-15
terminal	Sets terminal line parameters.	page 11-17

11.1.1 clrscr

▶ *MAC Extended ACL Config Commands*

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-ext-macl)#clrscr
RFS7000(config-ext-macl)#
```

11.1.2 deny

▶ MAC Extended ACL Config Commands

Use this command to specify packets that you want to reject.

NOTE Use a decimal value representation of ethertypes to implement a `permit/deny/mark` designation for a packet. The command set for Extended MAC ACLs provide the hexadecimal values for each listed ether type. The switch supports all ethertypes. Use the decimal equvilant of the ethertype listed or for any other type of ethertype.

Syntax

```
{deny}{any|host source MAC address|source MAC/source MAC address mask} {any|host
destination MAC address|destination MAC/destination MAC address mask}[vlan vlan-
id] [dot1p dot1p-value] [type value|ip|ipv6|arp|vlan|wisp | 0-65535] [log] [rule-
precedence access-list-entry precedence]
```

Parameters

Source Mask	Bit mask specifying the bits to match. Source wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Source MAC address and mask. • `any` – Any source host. • `host` – Exact source MAC address to match.
Destination Mask	Bit mask specifying the bits to match. Source wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Destination MAC address and mask. • `any` – Any destination host. • `host` – Exact destination MAC address to match.
dot1p<*0-7*>	802.1p priority value to match.
rule-precedence<*1-5000*>	Access-list entry precedence.
type(<*1-65535*>|arp|ip|ipv6|vlan|wisp)	Ether type value represented as integer or keywords for well-known ethertypes like IP, IPv6, ARP etc.
vlan<*1-4095*>	VLAN tag ID to match.

Usage Guidelines

The deny command disallows traffic based on layer 2 (data-link layer) information. The MAC access list denies traffic from a particular source MAC address or any MAC address. It also has an option to disallow traffic from a list of MAC addresses based on the source mask.

The MAC access list can be configured to disallow traffic based on VLAN information and ethernet type.

The most common ethernet type are:

- arp
- wisp

- ip
- 802.1q

By default, the switch does not allow layer 2 traffic to pass through the interface. To adopt access port through an interface, configure an access control list to allow an ethernet wisp.

NOTE A MAC access list entry to allow arp is mandatory to apply an IP based ACL to an interface. MAC ACL always takes precedence over IP based ACL's.

The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is allowed/denied based on the ACL configuration.

Example

The MAC AC (in the example below) denies traffic from any source MAC address to a particular host MAC address.

```
RFS7000(config-ext-macl)#deny any host 00:01:ae:00:22:11
RFS7000(config-ext-macl)#
```

The MAC ACL (in the example below) denies dot1q tagged traffic from VLAN interface 5.

```
RFS7000(config-ext-macl)#deny any any vlan 5 type 8021q
RFS7000(config-ext-macl)#
```

The example below denies traffic between two hosts based on MAC addresses.

```
RFS7000(config-ext-macl)#deny host 01:02:fe:45:76:89 host 01:02:89:78:78:45
RFS7000(config-ext-macl)#
```

11.1.3 end

▶ *MAC Extended ACL Config Commands*

Use this command to exit from the current mode and change to PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-ext-macl)#end
RFS7000#
```

11.1.4 exit

▶ *MAC Extended ACL Config Commands*

Use this command to end current mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-ext-macl)#exit
RFS7000(config)#
```

11.1.5 help

▶ MAC Extended ACL Config Commands

Use this command to access the system’s interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-ext-macl)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-ext-macl)#
```

11.1.6 mark

▶ *MAC Extended ACL Config Commands*

Use this command to specify a packet to mark.

☑ **NOTE** Use a decimal value representation of ethertypes to implement `permit/deny/mark` designations for a packet. The command set for an Extended MAC ACL provides the hexadecimal values for each of its listed ether types. The switch supports all ethertypes. Use the decimal equvilant of the ethertype listed in the CLI or for any other type of ethertype.

Syntax

```
{mark {dot1p <0-7>|tos <0-255>}}
{any|host source MAC address|source MAC source/MAC address mask}
{any|host destination MAC address|destination MAC/ destination MAC address mask}
[vlan vlan-id] [dot1p dot1p-value] [type value|ip|ipv6|arp|vlan| wisp|0-65535]
[log] [rule-precedence access-list-entry precedence]
```

Parameters

8021p<*0-7*>	Modifies the 802.1p VLAN user priority.
tos<*0-255*>	Modifies the TOS bits in an IP header.
Source MAC Address	Bit mask specifying the bits to match. The source wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Source MAC address and mask. • `any` – Any source host. • `host` – Exact source MAC address to match.
Destination MAC Address	Bit mask specifying the bits to match. The destination wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Destination MAC address and mask. • `any` – Any destination host. • `host` – Exact destination MAC address to match.
dot1p<*0-7*>	VLAN 802.1p priority value to match.
rule-precedence<*1-5000*>	Access-list entry precedence.
type(<*1-65535*>|arp|ip|ipv6|vlan|wisp)	Ethertype value represented as integer or keywords for well-known ethertypes like IP, IPv6, ARP etc.
vlan<*1-4095*>	The VLAN tag ID to match.

Usage Guidelines

Use the mark option to specify the t*ype of service* (tos) and priority value. The tos value is marked in the IP header and the 802.1p priority value is marked in the dot1q frame.

Whenever the interface receives the packet, its content is checked against all the ACE's in the ACL. It is marked based on the ACL configuration.

Example

The example below marks the dot1p priority value to 6 for all 802.1q tagged traffic from VLAN interface 5.

```
RFS7000(config-ext-macl)#mark 8021p 6 any any vlan 5 type 8021q
RFS7000(config-ext-macl)#
```

The example below marks the tos field to 254 for all IP traffic coming from the source MAC address.

```
RFS7000(config-ext-macl)#mark tos 254 host 00:33:44:55:66:77 any type ip
RFS7000(config-ext-macl)#
```

11.1.7 no

▶ *MAC Extended ACL Config Commands*

Use this command to negate a command or set defaults.

Syntax

```
no(deny|mark|permit)
```

This command negates all the syntax combinatins that you have used in *deny*, *mark* and *permit* to configure the Extended ACL.

Parameters

deny	Specifies packets to reject.
mark	Specifies packets to mark.
permit	Specifies packets to forward.

Example

```
RFS7000(config-ext-macl)#no mark tos 254 host 00:33:44:55:66:77 any type ip rule-
precedence 50
RFS7000(config-ext-macl)#

RFS7000(config-ext-macl)#no deny any any vlan 5 type 8021q rule-precedence 10
RFS7000(config-ext-macl)#

RFS7000(config-ext-macl)#no permit any any type wisp rule-precedence 50
RFS7000(config-ext-macl)#
```

11.1.8 permit

▶ *MAC Extended ACL Config Commands*

Use this command to specify packets to forward.

☑ **NOTE** Use a decimal value representation of ethertypes to implement permit/deny/mark designations for a packet. The command set an an Extended MAC ACL provides the hexadecimal values for each listed ethertype. The switch supports all ethertypes. Use the decimal equvilant of the ethertype listed in the CLI or for any other type of ethertype.

A MAC access list (to allow an arp) is mandatory for both port and WLAN ACL's.

Syntax

```
{permit} {any|host source MAC address|source MAC\source MAC address mask}
{any|host destination MAC address | destination MAC\destination MAC address mask}
[vlan vlan-id] [dot1p dot1p-value] [type value|ip|ipv6|arp| vlan|wisp|0-65535]
[log] [rule-precedence access-list-entry precedence]
```

Parameters

Source MAC Address	Bit mask specifying the bits to match. The source wildcard can be any one of the following. • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Source MAC address and mask. • `any` – Any source host. • `host` – Exact source MAC address to match.
Destination MAC Address	Bit mask specifying the bits to match. The destination wildcard can be any one of the following: • `xx:xx:xx:xx:xx:xx/xx:xx:xx:xx:xx:xx`–Destination MAC address and mask. • `any` – Any destination host. • `host` – Exact destination MAC address to match.
dot1p<*0-7*>	802.1p priority.
rule-precedence<*1-5000*>	Access-list entry precedence.
type(<*1-65535*>|arp|ip|ipv6|vlan|wisp)	EtherType.
vlan<*1-4095*>	VLAN ID.

Usage Guidelines

When creating a Port ACL, the switch by default does not permit an ethertype WISP. First create a rule to allow WISP to adopt access ports. Use the following CLI command to adopt access ports:

```
permit any any type wisp
```

NOTE Use the following command to attach a MAC access list to a port on a layer 2 interface:

```
mac access-group <acl number/name> in
```

The permit command in the MAC ACL disallows traffic based on layer 2 (data-link layer) information. MAC access list permits traffic from a source MAC address or any MAC address. It also has an option to allow traffic from a list of MAC addresses (based on the source mask).

The MAC access list can be configured to allow traffic based on VLAN information, ethernet type. Common ethernet types include:

- arp
- wisp
- ip
- 802.1q

The switch (by default) does not allow layer 2 traffic to pass through the interface. To adopt an access port through an interface, configure an access control list to allow ethernet wisp.

NOTE To apply an IP based ACL to an interface, a MAC access list entry to allow arp is mandatory. MAC ACL always takes precedence over IP based ACL's.

The last ACE in the access list is an implict deny statement.

Whenever the interface receives the packet, its content is checked against all the ACEs in the ACL. It is allowed/denied based on the ACL configuration.

Example

The example below permits wisp based traffic from any source MAC address to any destination MAC address.

```
RFS7000(config-ext-macl)#permit any any type wisp
RFS7000(config-ext-macl)#
```

The example below permits arp based traffic from any source MAC address to any destination MAC address.

```
RFS7000(config-ext-macl)#permit any any type arp
RFS7000(config-ext-macl)#
```

The example below permits IP based traffic from a particular source MAC address to any destination MAC address.

```
RFS7000(config-ext-macl)#permit host 11:22:33:44:55:66 any type ip
RFS7000(config-ext-macl)#
```

11.1.9 service

▶ *MAC Extended ACL Config Commands*

Use this command to invoke service commands to trobuleshoot or debug `(config-if)` instance configurations.

Syntax

```
service(clear|diag-shell|save-cli|show|start-shell|tethereal)
```

Parameters

clear	Removes specified support information.
diag-shell	Provides diagnostic shell access to debug and test the switch.
save-cli	Saves the CLI tree for all modes in html format.
show	Shows running system information.
start-shell	Provides shell access.

Example

```
RFS7000(config-ext-macl)#service diag-shell
Diagnostic shell started for testing
diag >
  boot              Reboots the switch
  delete            Deletes specified file from the system.
  exit              Exit from the CLI
  fallback          Configures firmware fallback feature
  help              Description of the interactive help system
  logout            Exit from the CLI
  no                Negate a command or set its defaults
  reload            Halt and perform a warm reboot
  service           Service Commands
  show              Show running system information
  upgrade           Upgrade firmware image
diag >

RFS7000(config-ext-macl)#service save-cli
 CLI command tree is saved as clitree.html.
 This tree can be viewed via web at http://<ipaddr>/cli/clitree.html
RFS7000(config-ext-macl)#

RFS7000(config-ext-macl)#service show ?
  cli                Show CLI tree of current mode
  command-history    Display command (except show commands) history.
  crash-info         Display information about core, panic and AP dump files
  info               Show snapshot of available support information
  last-passwd        Display last password used to enter shell
  reboot-history     Show reboot history
  startup-log        Show startup log
  upgrade-history    Show upgrade history
RFS7000(config-ext-macl)#service show

RFS7000(config-ext-macl)#service start-shell
Last password used: password with MAC 00:a0:f8:65:ea:8e
RFS7000(config-ext-macl)#
```

11.1.10 show

▶ *MAC Extended ACL Config Commands*

Use this command to view current system information.

Syntax

```
show<paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Usage Guidelines

The `show access-list` command displays the access lists configured for the switch. Provide the access list name or number to view specific ACL details.

Example

```
RFS7000(config-ext-macl)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

RFS7000(config-ext-macl)#show
```

```
RFS7000(config-ext-macl)#show access-list
Extended MAC access list 200
    permit any any type arp rule-precedence 10
    permit any any type wisp rule-precedence 20
Extended MAC access list 250
    deny host 01:02:fe:45:76:89 host 01:02:89:78:78:45 rule-precedence 10
    permit any any type arp rule-precedence 20
RFS7000(config-ext-macl)#
```

11.1.11 terminal

▶ *MAC Extended ACL Config Commands*

Use this command to set the length or number of lines displayed

Syntax

```
terminal(monitor|no)
terminal no(monitor)
```

Parameters

monitor	Copies debug output to the current terminal line.
no	Negates a command or sets defaults. • monitor – Copies debug output to the current terminal line.

Usage Guidelines

By default, log messages are generally not displayed over a Telnet session. Use the `terminal monitor` command to view t log messages using Telnet.

Example

```
RFS7000(config-ext-macl)#terminal monitor
RFS7000(config-ext-macl)#

RFS7000(config-ext-macl)#terminal no monitor
RFS7000(config-ext-macl)#
```

12

DHCP Instance

Use the `(config-dhcp)`instance to configure the DHCP server address pool associated the switch.

12.1 DHCP Config Commands

Table 12.1 summarizes `config-std-nacl` commands.

Table 12.1 Extended ACL Config Command Summary

Command	Description	Ref.
address	Configures DHCP server include range.	page 12-3
bootfile	Assigns a boot file name. The bootfile name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.	page 12-4
client-identifier	Use an ascii string as a client identifier.	page 12-5
client-name	Assigns an client name.	page 12-6
clrscr	Clears the display screen.	page 12-7
ddns	Configures Dynamic DNS.	page 12-8
default-router	Configures the default routers IP address.	page 12-9
dns-server	Configure the IP address for the DNS Server.	page 12-10
domain-name	Configure the domain name.	page 12-11
end	Ends the current mode and moves to the EXEC mode.	page 12-12

Command	Description	Ref.
exit	Ends the current mode and moves to the previous mode.	page 12-13
hardware-address	Configures the hardware address using either a dashed or dotted hexadecimal string.	page 12-14
help	Describes the interactive help system.	page 12-15
host	Configures the IP address for the host.	page 12-16
lease	Assigns the lease time for the dhcp IP address.	page 12-17
netbios-name-server	Configures NetBIOS (WINS) name servers.	page 12-18
netbios-node-type	Confiures NetBIOS node type.	page 12-19
network	Configures a network number and mask for the DHCP Server.	page 12-20
next-server	Configures the next server in boot process.	page 12-21
no	Negates a command or sets defaults.	page 12-22
option	Assigna a name for the DHCP option.	page 12-23
service	Displays the service commands for DHCP.	page 12-24
show	Displays current running system information.	page 12-25
update	Controls the usage of dynamic DNS.	page 12-27

12.1.1 address

▶ DHCP Config Commands

Use this command to specify a range of addresses for DHCP network pool.

Syntax

```
address (range) (low IP address) (high IP address)
```

Parameters

range (low IP address) (high IP address)	Use this commnad to add an address range for the DHCP server. • low IP address – The first ip address in the address range. • high IP address – The last ip address in the address range.

Usage Guidelines

Use the `address` comand to specify a range of addresses for the DHCP network pool. The DHCP server assigns IP address to DHCP clients from the address range. A high IP address is the upper limit for providing the IP address and low IP address is the lower limit for providing the IP address.

Use the `no address (range)` command to remove the DHCP address range.

Example

```
RFS7000(config-dhcp)#address range 2.2.2.2 2.2.2.50
RFS7000(config-dhcp)#
```

12.1.2 bootfile

▶ *DHCP Config Commands*

Use this command to assign a bootfile name for the DHCP configuration on the network pool.

Syntax

```
bootfile <filename>
```

Parameters

bootfile <filename>	Indicates the boot image for bootp clients. The file name can contain letters, numbers, dots and hyphens. Consecutive dots and hyphens are not permitted.

Usage Guidelines

Use the `bootfile` command to specify the boot image. The boot file contains the boot image name used for booting the bootp clients (DHCP clients).

Example

```
RFS7000(config-dhcp)#bootfile bootexample.txt
RFS7000(config-dhcp)#
```

12.1.3 client-identifier

▸ *DHCP Config Commands*

Use this command to assign a name to the client-identifier. A client identifier is used to reserve an IP address for DHCP clients.

Syntax

```
client-identifier <ascii string>
```

Parameters

client-identifier <ascii string>	To prepend a null character , use `\\0` at beginning. A single `\` in the input is ignored.

Example

```
RFS7000(config-dhcp)#client-identifier testid
RFS7000(config-dhcp)#
```

12.1.4 client-name

▶ *DHCP Config Commands*

Use this command to a add client name for the DHCP clients.

Syntax

```
client-name <name>
```

Parameters

client-name <name>	Use `client-name` to add a client name. Domain name must not be included.

Example

```
RFS7000(config-dhcp)#client-name testpc
RFS7000(config-dhcp)#
```

12.1.5 clrscr

▶ *DHCP Config Commands*

Use this command to clear the screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-dhcp)#clrscr
RFS7000(config-dhcp)#
```

12.1.6 ddns

▶ *DHCP Config Commands*

Use this command to configure dynamic DNS parameters like domain name, enabling multi-user class and IP address of the server.

Syntax

```
ddns [domainname (name)|multiple-user-class|server (IP address) (IP address)|
ttl <1-864000>|update-all]
```

Parameters

domainname (name)	Sets domain name used for DDNS updates.
multiple-user-class	Enables multiple user class option.
server (IP address) (IP address)	Specifiies the server to which DDNS updates have been sent. • ip address – IP address in dotted decimal format. • ip address – IP address in dotted decimal format.
ttl <1-864000>	Configures time to live (TTL) value used for DDNS updates. • <1-864000> – TTL value in seconds
update-all	Sends manual DDNS updates for all valid DHCP leases.

Usage Guidelines

A DHCP client may not perform updates for RR's A, TXT and PTR. Use `update (dns) (override)` to enable the internal DHCP server to send DDNS updates for resource records (RR's) A, TXT and PTR. The DHCP server can always override the client even if the client is configured to perform the updates.

In the network pool of DHCP server, FQDN is configured as DDNS domain name. This is used internally in the DHCP packets between DHCP server available on the switch and DNS server.

Example

```
RFS7000(config-dhcp)#ddns domainname TestDomain.com
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#ddns multiple-user-class
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#ddns ttl 1000
RFS7000(config-dhcp)#

RFS7000(config-dhcp)#ddns update-all
RFS7000(config-dhcp)#
```

12.1.7 default-router

▶ *DHCP Config Commands*

Use this command to configure the default router or gateway IP address for the network pool. To remove the default router list, use the `no default-router` command.

```
default-router <Router IP address>
```

Parameters

default-router <router IP address>	Specifies the default router IP address for the network pool. • <router IP address> – Router's IP address.

Usage Guidelines

The IP address of the router should be on the same subnet as the client subnet.

Example

```
RFS7000(config-dhcp)#default-router 2.2.2.1
RFS7000(config-dhcp)#
```

12.1.8 dns-server

DHCP Config Commands

Use this command to configure the DNS server’s IP address available to all the DHCP clients connected to the pool. Use the `no dns-server` command to remove DNSserver list.

Syntax

```
dns-server <ip address1> <ip address2> <ip address3> .....<ip address8>
```

Parameters

dns-server <IP address>	Configures the DNS Server’s IP address. • <IP address> – Server's IP address.

Usage Guidelines

For DHCP client’s, the DNS server’s IP address is used to map the host name to IP address. The DHCP client uses the DNS servers IP address based on the order (sequence) it is configured.

Example

```
RFS7000(config-dhcp)#dns-server 2.2.2.222
RFS7000(config-dhcp)#
```

12.1.9 domain-name

▶ *DHCP Config Commands*

Use this command to configure the domain name for the network pool. Use the `no domain-name` command to remove the domain name.

Syntax

```
domain-name (name)
```

Parameters

domain-name (name)	Configures the domain name for the network pool.

Usage Guidelines

The doamin name can not be more than 256 characters.

Example

```
RFS7000(config-dhcp)#domain-name Engineering
RFS7000(config-dhcp)#
```

12.1.10 end

▶ *DHCP Config Commands*

Use this command to exit from the current mode and change to PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-dhcp)#end
RFS7000#
```

12.1.11 exit

▶ *DHCP Config Commands*

Use this command to end the current mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config)#ip dhcp pool TestPool
RFS7000(config-dhcp)#exit
RFS7000(config)#
```

12.1.12 hardware-address

▶ *DHCP Config Commands*

Use this command to reserve IP address (manually) based on a DHCP client's hardware address. Use the `no hardware-address` command to remove this form the DHCP pool.

Syntax

```
hardware-address [XX-XX-XX-XX-XX-XX | XX:XX:XX:XX:XX:XX]
```

Parameters

hardware-address [XX-XX-XX-XX-XX-XX | XX:XX:XX:XX:XX:XX]	Configures the client's hardware address. • XX-XX-XX-XX-XX-XX – Dashed-hexadecimal string. • XX:XX:XX:XX:XX:XX – Dotted-hexadecimal string.

Usage Guidelines

This command accepts only hexadecimal values.

Example

```
RFS7000(config-dhcp)#hardware-address 00:01:23:45:32:22
RFS7000(config-dhcp)#
```

12.1.13 help

▶ *DHCP Config Commands*

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-dhcp)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-dhcp)#
```

12.1.14 host

▶ *DHCP Config Commands*

Use this command to configure a fixed IP address for the host in dotted decimal format. Use the `no host` command to remove the host from the DHCP pool.

Syntax

```
host <IP address>
```

Parameters

host <IP address>	Fixed address for host. • IP address – IP address in dotted decimal format.

Usage Guidelines

The DHCP host pool (used to manually assign specify IP address based on hardware address/client identifier), configuration must contain a host IP address, client name and hardware address/client identifier.

The host IP address must belong to any subnet that exisits on the switch. There must be a DHCP network pool corresponding to that host IP address. There is no limit on the number of manual bindings but you can configure only one manual binding per host pool.

Example

```
RFS7000(config-dhcp)#host 2.2.2.111
RFS7000(config-dhcp)#
```

12.1.15 lease

▶ *DHCP Config Commands*

Use this command to configure a valid lease time for the IP address used by all DHCP clients in the network pool.

Syntax

```
lease [{<0-365> <0-23> <0-59>}|infinite]
```

Parameters

lease [{<0-365> <0-23> <0-59>} |infinite]	Sets the lease time for IP address. • <0-365> – Lease period in days. Days can be made as 0 only when hours and/or mins are greater than 0. • <0-23> – Used with the above to set the hours for the lease period. • <0-59> – Used with the above to set the minutes for the lease period. • infinite – Sets the lease period as infinite.

Usage Guidelines

If lease parameter is not configured on the DHCP network pool, the default value is used. The default value of the lease is 24 hours.

The lease vlaue for DHCP host pool is infinite.

Example

```
RFS7000(config-dhcp)#lease 20 12 30
RFS7000(config-dhcp)#
```

12.1.16 netbios-name-server

▶ *DHCP Config Commands*

Use this command to configure the netbios-name server’s IP address.

Syntax

```
netbios-name-server <IP address>
```

Parameters

netbios-name-server <IP address>	NetBIOS (WINS) name servers. • <IP address> – NetBIOS name server's IP address.

Example

```
RFS7000(config-dhcp)#netbios-name-server 2.2.2.222
RFS7000(config-dhcp)#
```

12.1.17 netbios-node-type

▶ *DHCP Config Commands*

Use this command to configure the netbios-node type.

Syntax

```
netbios-node-type [b-node|h-node|m-node|p-node]
```

Parameters

netbios-node-type [b-node | h-node | m-node | p-node]	NetBIOS (WINS) name servers. • b-node – Broadcast node. • h-node – Hybrid node. • m-node – Mixed node. • p-node – Peer-to-peer node.

Example

```
RFS7000(config-dhcp)#netbios-node-type p-node
RFS7000(config-dhcp)#
```

12.1.18 network

▶ *DHCP Config Commands*

Use this command to configure the network pool’s IP address. This will map the current DHCP pool with the specific network.

Syntax

```
network [A.B.C.D|A.B.C.D/M]
```

Parameters

network [A.B.C.D|A.B.C.D/M]	Network number and mask. • A.B.C.D – Network number in dotted decimal format. • A.B.C.D/M – Network number and mask.

Usage Guidelines

Ensure a VLAN interface with specific network /subnet exists on the switch before mapping the DHCP pool to a particular network.

Example

```
RFS7000(config-dhcp)#network  2.2.2.0/24
RFS7000(config-dhcp)#
```

12.1.19 next-server

▶ *DHCP Config Commands*

Use this command to configure the IP address of the next server in the boot process.

Syntax

```
next-server <IP address>
```

Parameters

next-server <IP address>	Next server in boot process. • <IP address> – Server's IP address.

Example

```
RFS7000(config-dhcp)#next-server 2.2.2.22
RFS7000(config-dhcp)#
```

12.1.20 no

▶ *DHCP Config Commands*

Use this command to negate a command or set defaults.

Syntax

```
no [address|bootfile|client-identifier|client-name|ddns|default-router|dns-
server|domain-name|hardware-address|host|lease|netbios-name-server|netbios-node-
type|network|next-server|option|update]
```

Parameters

The no command negates any command associated with it. Wherever required, use the same parameters associated with the command getting negated.

Example

```
RFS7000(config)#no ip dhcp pool hotpool
RFS7000(config)#

RFS7000(config)#no ip dhcp pool test
RFS7000(config)#

RFS7000(config-dhcp)#no update dns
RFS7000(config-dhcp)#
```

12.1.21 option

▶ *DHCP Config Commands*

Use this command to define the raw DHCP option used in DHCP pools.

Syntax

```
option (name)
```

Parameters

option (name)	Raw DHCP options. • (name) – Name of the DHCP option.

Usage Guidelines

Used to define non standard DHCP options option-code (0-254).

Example

```
RFS7000(config)#ip dhcp option option189 189 ascii
RFS7000(config)#
```

12.1.22 service

DHCP Config Commands

Use this command to invoke service commands to trobuleshoot or debug the `(config-dhcp)` instance configurations.

Syntax

```
service(show) (cli)
```

Parameters

show	Shows running system information.
cli	Shows CLI tree of current mode.

Example

```
RFS7000(config-dhcp)#service show cli
DHCP Server Config mode:
+-address
  +-range
    +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
      +-A.B.C.D [address range A.B.C.D ( A.B.C.D |)]
+-bootfile
  +-WORD [bootfile WORD]
+-client-identifier
  +-WORD [client-identifier WORD]
+-client-name
  +-WORD [client-name WORD]
+-clrscr [clrscr]
+-ddns
  +-domainname
    +-WORD [ddns domainname WORD]
  +-multiple-user-class [ddns multiple-user-class]
  +-server
    +-A.B.C.D [ddns server A.B.C.D (A.B.C.D|)]
      +-A.B.C.D [ddns server A.B.C.D (A.B.C.D|)]
  +-ttl
    +-<1-864000> [ddns ttl <1-864000>]
  +-update-all [ddns update-all]
+-default-router
  +-A.B.C.D [default-router .A.B.C.D]
+-dns-server
  +-A.B.C.D [dns-server .A.B.C.D]
+-do
  +-LINE [do LINE]
+-domain-name
  +-WORD [domain-name WORD]
+-end [end]
+-exit [exit]
+-hardware-address
  +-XX-XX-XX-XX-XX-XX [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-XX-
XX)(ethernet|token-ring|)]
    +-ethernet [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-XX-
XX)(ethernet|token-ring|)]
    +-token-ring [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-XX-
XX)(ethernet|token-ring|)]
  +-XX:XX:XX:XX:XX:XX [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-XX-
XX)(ethernet|token-ring|)]
    +-ethernet [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-XX-
XX)(ethernet|token-ring|)]
    +-token-ring [hardware-address (XX:XX:XX:XX:XX:XX|XX-XX-XX-XX-XX-
XX)(ethernet|token-ring|)]
RFS7000(config-dhcp)#
```

12.1.23 show

▶ DHCP Config Commands

Use this command to view current system information.

Syntax

```
show <paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Example

```
RFS7000(config-dhcp)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                Encryption related commands
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Internet Protocol (IP)
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         spanning-tree Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
RFS7000(config-dhcp)#show
```

```
RFS7000(config)#show dhcp config

service dhcp
ip dhcp option option189 189 ascii
!
ip dhcp pool vlan4
 default-router 2.2.2.1
 network 4.4.4.0/24
 address range 4.4.4.100 4.4.4.200
!
ip dhcp pool vlan2
!
ip dhcp pool TestPool
 lease 200 12 30
 domain-name TestDomain
 bootfile DHCPbootfile
 netbios-node-type p-node
 ddns domainname TestDomain
 address range 1.2.3.2 2.3.2.1

RFS7000(config)#show dhcp status

DHCP Server is Running on following interfaces

        vlan4

RFS7000(config)#


RFS7000(config)#show ip dhcp binding
IP              MAC/Client-Id      Type       Expiry Time
--              -------------      ----       -----------
RFS7000(config)#
```

12.1.24 update

▶ *DHCP Config Commands*

Use this command to control the usage of the DDNS service.

Syntax

```
update (dns)(override)
```

Parameters

update (dns) (override)	Controls the usage of the DDNS service. • (dns) – Dynamic DNS Configuration. • (override) – Enable Dynamic Updates by onboard DHCP Server.

Usage Guidelines

A DHCP client may not perform updates for RR's A, TXT and PTR. Use `update (dns) (override)` to enable the internal DHCP Server to send DDNS updates for resource records (RR's) A, TXT and PTR. The DHCP Server can always override the client, even if the client is configured to perform the updates.

In the network pool of DHCP Server, FQDN is configured as DDNS domain name. This is used internally in DHCP packets between the switch's DHCP Server and the DNS server.

Example

```
RFS7000(config-dhcp)#update dns override
RFS7000(config-dhcp)#
```

12.2 Configuring DHCP Server using CLI

DHCP configuration is accomplished by creating pools and mapping them to L3 interfaces (SVI).

A pool can be configured either as a network pool or host pool. A network pool includes ranges. When the network pool is mapped to a L3 interface, DHCP clients requesting IP from the interface get an IP from the included range. A host pool is used to assign static/fixed IP address to DHCP clients.

12.2.1 Creating network pool

```
RFS7000(config)#ip dhcp pool test

RFS7000(config-dhcp)#network 192.168.0.0/24

RFS7000(config-dhcp)#address range 192.168.0.30 192.168.0.60

RFS7000(config-dhcp)#domain-name test.com

RFS7000(config-dhcp)#dns-server 192.168.0.10 192.168.0.11

RFS7000(config-dhcp)#lease 10

RFS7000(config-dhcp)#exit

RFS7000(config)#ip dhcp restart
```

12.2.2 Creating host pool

```
RFS7000(config)#ip dhcp pool hostpool

RFS7000(config-dhcp)#client-name linuxbox

RFS7000(config-dhcp)#host 192.168.0.50

RFS7000(config-dhcp)#hardware 00:a0:f8:6f:6b:88

RFS7000(config-dhcp)#exit

RFS7000(config)#ip dhcp restart
```

12.2.3 Troubleshooting DHCP configuration

All DHCP Server configurations come into effect only after rebooting the DHCP Server. Execute the `ip dhcp restart`, at a global level, to restart the DHCP Server. The following steps help setup/troubleshoot DHCP related configuration issues:

1.To change the domain name for a pool from its exiting name to `test1`:

```
RFS7000(config)#ip dhcp pool test

RFS7000(config-dhcp)#domain-name example.com

RFS7000(config-dhcp)#exit

RFS7000(config)#ip dhcp restart
```

2. A DHCP reboot is required to implement the configuration made at both levels — the DHCP pool context level and DHCP global context level. The following example defines the need to reboot the DHCP Server to implement changes at the global level:

   ```
   RFS7000(config)#ip dhcp excluded-address 192.168.0.20 192.168.0.30
   RFS7000(config)#ip dhcp restart
   ```

> ✓ **NOTE** To avoid multiple e DHCP Server requests, restart the DHCP Server only after making all the required updates.

3. Use the `network` CLI command to map the network pool to interface.

   ```
   network 192.168.0.0/24
   ```

   In the above example, 192.168.0.0/24 represents the L3 interface. When executing this command, no check is performed to endorse whether any interface with the specified IP/Netmask exists. The verification is not performed because you can create a pool and map it to non existing L3 interface.

   Later (when you add a L3 interface and assign an IP address to it), the DHCP Server gets enabled/started on the interface. If you have a pool for 192.168.0.0/24, but the L3 interface is 192.168.0.0/16, DHCP wont be enabled on 192.168.0.0/16, as it is different from 192.168.0.0/24.

4. A network pool without any include range is as good as not having a pool at all. Add an include range using the `address range` CLI command

   ```
   address range 192.168.0.30 192.168.0.30
   ```

5. To work properly, a host pool should have the following 3 items configured.

   - client-name (CLI is `client-name <name>`)
   - fixed-address (CLI is `host <ip>`)
   - hardware-address/client-identifier

     CLI for hardware address is `hardware-address <addr>`

     CLI for client-identifier is `client-identifier <id>`

   If using `client-identifier` instead of `hardware-address,` the DHCP client sends the client-identifier when it requests for IP address.

6. A host pool should have its corresponding network pool configured otherwise the host pool will be rendered useless. The fixed IP address configured in the host pool must be in the subnet of the corresponding network pool.

7. Use the global configuration mode `service dhcp` to enable/disable the DHCP Server. This enables/disables the DHCP Server on all interfaces.

8. If you create a pool and map it to interface, it automatically gets enabled, provided DHCP is enabled at global level. Use the `no network` command to disable DHCP on a per pool/interface basis.

9. To add a newly created pool to the network pool, use one of the following:

   - `network ( Eg network 192.168.0.0/24 )`
   - `address range   ( Eg address range 192.168.0.30 192.168.0.50 )`

10. To add a newly created pool to host pool, use one of the following:

    - `host ( Eg host 192.168.0.1 )`
    - `client-name ( Eg client-name "kaveri" )`
    - `client-identifier ( Eg client-identifier "aabb:ccdd" )`
    - `hardware-address ( Eg hardware-address aa:bb:cc:dd:ee:ff )`

11. A pool can be configured as the host pool or network pool, but not both.
12. A host pool can have either `client-identifier` or `hardware-address` configured, but not both.
13. An excluded address range has higher precedence then an included address range. If a range is part of both an excluded and included address range, it will be excluded.
14. DHCP options are first defined at the global level, using `ip dhcp option <name> <code> <type>`. The value for these options are associated using the `option` which is under DHCP pool context.

13

RADIUS Server Instance

The **`radius-server local`** command takes you to the RADIUS server mode. Local (Onboard) RADIUS server configuration commands are listed under this mode. Use the **`(config-radsrv)`**instance to configure local RADIUS server parameters.

13.1 RADIUS Configuration Commands

Table 13.1 summarizes the Gloabl Config commands.

Table 13.1 Extended ACL Config Command Summary

Command	***Description***	***Ref.***
authentication	RADIUS authentication.	page 13-3
ca	Configures ca certificate parameters.	page 13-4
clrscr	Clears the display screen.	page 13-5
crl-check	Certificate Revocation List (CRL) check.	page 13-6
end	Ends the current mode and moves to the EXEC mode.	page 13-7
exit	Ends the current mode and moves to the previous mode.	page 13-8
group	Configures RADIUS user group paramaters. **NOTE** Creates another sub-instance called **`config-radsrv-group`** with its own command summary.	page 13-9
help	Describes the interactive help system.	page 13-19

Command	**Description**	**Ref.**
ldap-server	LDAP server parameters.	page 13-20
nas	RADIUS client.	page 13-22
no	Negates a command or set its defaults.	page 13-23
proxy	RADIUS proxy server.	page 13-24
rad-user	RADIUS user configuration.	page 13-25
server	Configures server certificate parameters.	page 13-26
service	Service commands.	page 13-27
show	Shows running system information.	page 13-28

13.1.1 authentication

▶ *RADIUS Configuration Commands*

Use this command to configure authentication used with RADIUS server.

Syntax

```
authentication(data-source|eap-auth-type)
authentication data-source(ldap|local)
authentication eap-auth-type(all|peap-gtc|peap-mschapv2|tls|ttls-md5|
ttls-mschapv2|ttls-pap)
```

Parameters

data-source	RADIUS data source for user authentication. • ldap – Remote LDAP server. • local – Local user database.
eap-auth-type	RADIUS EAP and default authentication type configuration. • all – Enable both ttls and peap. • peap-gtc – Eap type peap with default auth type gtc. • peap-mschapv2 – Eap type peap with default auth type mschapv2. • tls – Eap type tls. • ttls-md5 – EAP type ttls with default auth type md5. • ttls-mschapv2 – EAP type ttls with default auth type mschapv2. • ttls-pap – EAP type ttls with default auth type pap.

Usage Guidelines

Set `eap-auth-type` to `all` to service any RADIUS request received from mobile unit. Setting `eap-auth-type` to `peap-gtc/ peap-mschapv2` ensure `peap-gtc/peap-mschapv2` service only.

Similarly, set `eap-auth-type` to `ttls-md5/ttls-mschapv2/ttls-pap` to service all the ttls based authentication RADIUS request from the mobile unit.

Setting `eap-auth-type` to `tls` ensures only tls authentication type are serviced.

Example

```
RFS7000(config-radsrv)#authentication eap-auth-type peap-mschapv2
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#authentication data-source ldap
RFS7000(config-radsrv)#
```

13.1.2 ca

▶ *RADIUS Configuration Commands*

Use this command to configure CA (Certificate Authority) parameters.

Syntax

```
ca trust-point(WORD)
```

Parameters

trust-point (WORD)	Trust point configuration. • WORD – Existing trust point name.

Usage Guidelines

Configure the trustpoint used by the local RADIUS server. Create the **`trustpoint`** before it is used by the **`crypto pki trustpoint`** command.

The default trust point in use is – `default-trustpoint.`

Example

In the example below, the trustpoint (`tp1)` already has a certificate associated with it.

```
RFS7000(config)#radius-server local
RFS7000(config-radsrv)#ca trust-point tp1
RFS7000(config-radsrv)#
```

13.1.3 clrscr

▶ *RADIUS Configuration Commands*

Use this command to clear the screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-radsrv)#clrscr
RFS7000(config-radsrv)#
```

13.1.4 crl-check

▶ *RADIUS Configuration Commands*

Use this command to enable a *Certificate Revocation List* (CRL) check. To enable the certificate revocation list, ensure `crl list` is loaded using the **`crypto pki import <trustpoint-name> crl`** command.

Syntax

```
crl-check
```

Parameters

enable	Enables a CRL check.

Usage Guidelines

Authentication type `tls` uses certificates for authentication. CRL, updated with a trustpoint, has index numbers of revoked certifcates. CRL checks for any revoked certificates used for `tls` authentication.

Example

```
RFS7000(config-radsrv)#crl-check enable
RFS7000(config-radsrv)#
```

13.1.5 end

▶ *RADIUS Configuration Commands*

Use this command to exit from the current mode and change to the PRIV EXEC mode. The prompt now changes to **RFS7000#**.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-radsrv)#end
RFS7000#
```

13.1.6 exit

▶ *RADIUS Configuration Commands*

Use this command to exit current mode and move to the previous mode (GLOBAL-CONFIG). The prompt changes to **RFS7000(config)#**.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-radsrv)#exit
RFS7000(config)#
```

13.1.7 group

▶ *RADIUS Configuration Commands*

Use this command to configure RADIUS user groups. The CLI moves to a sub-instance **`config-radsrv-group`**, to create a new group.

The prompt changes from **`RFS7000(config-radsrv)#`** to **`RFS7000(config-radsrv-group)#`**.

Table 13.2 summarizes the RADIUS User Group commands within **`(config-radsrv-group)`** sub-instance.

Table 13.2 RADIUS User Group Configuration Command Summary

Command	***Description***	***Ref.***
clrscr	Clears the display screen.	page 13-9
end	Ends the current mode and changes to the EXEC mode.	page 13-10
exit	Ends the current mode and moves to the previous mode.	page 13-10
group	Configure RADIUS user group paramaters.	page 13-10
guest-group	Guest group configuration.	page 13-11
help	Describes o the interactive help system.	page 13-11
no	Negates a command or set its defaults.	page 13-11
policy	RADIUS group access policy configuration.	page 13-12
rad-user	Adds a RADIUS user to a group.	page 13-14
service	Service Commands.	page 13-14
show	Shows running system information.	page 13-15

13.1.7.1 clrscr

▶ *RADIUS Configuration Commands*

Use this command to clear the display screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-radsrv-group)#clrscr
RFS7000(config-radsrv-group)#
```

13.1.7.2 end

▶ *RADIUS Configuration Commands*

Use this command to exit from the current mode and move to the PRIV EXEC mode. The prompt changes to **RFS7000#**.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-radsrv-group)#end
RFS7000#
```

13.1.7.3 exit

▶ *RADIUS Configuration Commands*

Use this command to exit the current mode and move to the previous mode `(config-radsrv)`). The prompt changes to **RFS7000(config)#**.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-radsrv-group)#exit
RFS7000(config-radsrv)#
```

13.1.7.4 group

▶ *RADIUS Configuration Commands*

Use this command to configure RADIUS user group paramaters. This command creates a group within the exisitng RADIUS group.

Syntax

```
group
```

Parameters

WORD	RADIUS group name.

Example

```
RFS7000(config-radsrv)#group TestGroup
RFS7000(config-radsrv-group)#
```

13.1.7.5 guest-group

▶ *RADIUS Configuration Commands*

Use this command to manage a guest-user linked with hotspot. Create a guest-user and associate it with the guest-group. The guest-user and the policies of the guest-group is used for hotspot authentication/ authorization.

Syntax

```
guest-group
```

Parameters

enable	Enables this group as guest group.

Usage Guidelines

Use this command to create a guest group. The guest user created using `rad-user` must only be part of the guest group.

Example

```
RFS7000(config-radsrv-group)#guest-group enable
RFS7000(config-radsrv-group)#
```

13.1.7.6 help

▶ *RADIUS Configuration Commands*

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-radsrv-group)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-radsrv-group)#
```

13.1.7.7 no

▶ *RADIUS Configuration Commands*

Use this command to negate a command or set defaults.

Syntax

```
no(policy|rad-user|service)
no policy(day|time|vlan|wlan)
no policy wlan(<1-32>|all)<1-32>
```

Parameters

policy	RADIUS group access policy configuration.
day	Resets access policy day for this group.
time	Configures access policy time for this group.
vlan	VLAN ID for this group.
wlan	Configures WLAN access policy for this group.
<1-32>	WLAN Range.
all	Removes allowed WLANs.
rad-user	Removes users from this group.
WORD	Existing user name in this group.
all	Removes all users from this group.
service	Service commands.
radius	Disables the RADIUS Server.

Example

```
RFS7000(config-radsrv-group)#no policy day
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#no policy time
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#no policy vlan
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#no policy wlan 2 5
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#no rad-user all
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#no service radius
%%Info: Radius service stopped...
RFS7000(config-radsrv-group)#
```

13.1.7.8 policy

▶ *RADIUS Configuration Commands*

Use this command to configure the authorization policies for a particular group, like day/time of access, wireless LAN allowed to access and to set user based VLAN .

✓ **NOTE** User based VLAN is effective only if dynamic VLAN authorization is enabled on the wireless LAN page.

Syntax

```
policy(day|time|vlan|wlan)
policy day(all|fr|mo|sa|su|th|tu|we|weekdays)
ploicy time(start|end)<0-23><0-59>
policy vlan<1-4094>
```

Parameters

day	Day of access policy configuration.
all	All days (from Sunday to Saturday).
fr	Friday
mo	Monday
sa	Saturday
su	Sunday
th	Thursday
tu	Tuesday
we	Wednesday
weekdays	Allows access only in week days (Mo-Fr).
time	Configures time of access policy for this group.
start	Start time.
end	End time must be greater than the start time.
<0-23>	hour (hh) limit.
<0-59>	mins (mm) limit.
vlan	VLAN ID for this group.
<1-4094>	VLAN range.
wlan	Configure WLAN access policy for this group.
<1-32>	WLAN index.

Example

```
RFS7000(config-radsrv-group)#policy day weekdays
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#policy time start 12 12 end 22 22
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#policy vlan 20
RFS7000(config-radsrv-group)#

RFS7000(config-radsrv-group)#policy wlan 20 21 22 23
RFS7000(config-radsrv-group)#
```

13.1.7.9 rad-user

▶ *RADIUS Configuration Commands*

Use this command to add an exisitng RADIUS user to this group.If the RADIUS user is not available in the Onboard RADIUS server's database, create a new RADIUS user using `rad-user` command from **(config-radsrv)** mode. For more details check *13.1.13 rad-user* on page 25.

Syntax

```
rad-user
```

Parameters

WORD	Existing RADIUS user name.

Example

```
RFS7000(config-radsrv)#rad-user user1 password user1
RFS7000(config-radsrv)#group group1
RFS7000(config-radsrv-group)#rad-user user1
RFS7000(config-radsrv-group)#
```

13.1.7.10 service

▶ *RADIUS Configuration Commands*

Use this command to invoke RADIUS service commands, if they have been stopped. This command is used to enable the RADIUS Server. A service RADIUS restart is executed only from the **config** mode.

Syntax

```
service (show) (cli)
```

Parameters

show (cli)	Shows running system information.

Example

```
RFS7000(config-radsrv-group)#service show cli
Radius user group configuration mode:
+-clrscr [clrscr]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-group
  +-WORD [group WORD]
+-guest-group
  +-enable [guest-group enable]
+-help [help]
+-no
  +-policy
    +-day [no policy day]
    +-time [no policy time]
    +-vlan [no policy vlan]
    +-wlan
      +-<1-256> [no policy wlan (all|.<1-256>) ]
      +-all [no policy wlan (all|.<1-256>) ]
  +-rad-user
    +-WORD [no rad-user (all|WORD)]
    +-all [no rad-user (all|WORD)]
+-policy
  +-day
    +-all [policy day (all|weekdays|{mo|tu|we|th|fr|sa|su})]
    +-fr [policy day (all|weekdays|{mo|tu|we|th|fr|sa|su})]
    +-mo [policy day (all|weekdays|{mo|tu|we|th|fr|sa|su})]
    +-sa [policy day (all|weekdays|{mo|tu|we|th|fr|sa|su})]
    +-su [policy day (all|weekdays|{mo|tu|we|th|fr|sa|su})]
    +-th [policy day (all|weekdays|{mo|tu|we|th|fr|sa|su})]
    +-tu [policy day (all|weekdays|{mo|tu|we|th|fr|sa|su})]
    +-we [policy day (all|weekdays|{mo|tu|we|th|fr|sa|su})]
    +-weekdays [policy day (all|weekdays|{mo|tu|we|th|fr|sa|su})]
  +-time
    +-start
      +-<0-23>
        +-<0-59>
          +-end
            +-<0-23>
              +-<0-59> [policy time start <0-23> <0-59> end <0-23> <0-59>]
 -- MORE --, next page: Space, next line: Enter, quit: Control-C

RFS7000(config-radsrv-group)#
```

13.1.7.11 show

▶ *RADIUS Configuration Commands*

Use this command to view the current system information.

Syntax

```
show<paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command. For additional information, refer to *radius* and *show*.

Example

```
RFS7000(config-radsrv-group)#show ?
  access-list          Internet Protocol (IP)
  alarm-log            Display all alarms currently in the system
  autoinstall          autoinstall configuration
  banner               Display Message of the Day Login banner
  boot                 Display boot configuration.
  clock                Display system clock
  commands             Show command lists
  crypto               crypto
  debugging            Display debugging setting
  environment          show environmental information
  file                 Display filesystem information
  ftp                  Display FTP Server configuration
  history              Display the session command history
  interfaces           Interface status and configuration
  ip                   Internet Protocol (IP)
  ldap                 ldap server
  licenses             Show any installed licenses
  logging              Show logging configuration and buffer
  mac                  Media Access Control
  management           Display L3 Managment Interface name
  mobility             Display Mobility Parameters
  ntp                  Network time protocol
  password-encryption  password encryption
  privilege            Show current privilege level
  radius               Radius configuration commands
  redundancy-group     Display redundancy group parameters
  redundancy-history   Display state transition history of the switch.
  redundancy-members   Display redundancy group members in detail
  running-config       Current Operating configuration
  securitymgr          Display debug info for ACL, VPN and NAT
  sessions             Display current active open connections
  snmp                 Display SNMP engine parameters
  snmp-server          Display SNMP engine parameters
  startup-config       Contents of startup configuration
  terminal             Display terminal configuration parameters
  timezone             Display timezone
  upgrade-status       Display last image upgrade status
  users                Display information about terminal lines
  version              Display software & hardware version
  wireless             Wireless configuration commands

RFS7000(config-radsrv-group)#

RFS7000(config)#show radius trust-point

Trust-point Configured For Radius
________________________________
        Server Trust-point : tp1
        CA Trust-point     : default-trustpoint



RFS7000(config)#show radius configuration

Radius Server Configuration
---------------------------
         Server Status : enabled
         Data Source   : local

RFS7000(config)#
```

13.1.7.12 Example–Creating a Group

The use of the **`(config-radsrv-group)`** sub-instance is explained below:

1. Create a group called **Sales** in the local RADIUS Server database.

   ```
   RFS7000(config-radsrv)#group sales
   ```

2. Check the RADIUS user group configuration commands.

   ```
   RFS7000(config-radsrv-group)#?
   Radius user group configuration commands:
     clrscr       Clears the display screen
     end          End current mode and change to EXEC mode
     exit         End current mode and down to previous mode
     group        Configure radius user group paramaters
     guest-group  Guest group configuration
     help         Description of the interactive help system
     no           Negate a command or set its defaults
     policy       Radius group access policy configuration
     rad-user     Add Radius user to this group
     service      Service Commands
     show        Show running system information
   ```

3. Use the **`policy`** command to configure the group policies for the group created in Step 1.

   ```
   RFS7000(config-radsrv-group)#policy ?
   day   Day of access policy configuration
   time  Configure time of access policy for this group
   vlan  VLAN id for this group
   wlan  Configure wlan access policy for this group
   RFS7000(config-radsrv-group)#policy day weekdays
   RFS7000(config-radsrv-group)#policy time start 12 30 end 15 30
   ```

4. Use the **`policy vlan`** command to assign an VLAN ID of 10 to group Sales.

   ```
   RFS7000(config-radsrv-group)#policy vlan 10
   ```

5. Use the **`policy wlan`** command to allow only authorised users to access this groups wlan.

   ```
   RFS7000(config-radsrv-group)#policy wlan 1 2 5
   ```

6. Use `(config-radsrv)#rad-user` to create a user called **testuser** and add it to group **Sales**.

   ```
   RFS7000(config-radsrv)#rad-user testuser password testpassword group sales
   Sep 08 17:41:55 2006: RADCONF: Adding user "testuser" into local database
   Sep 08 17:41:55 2006: RADCONF: User "testuser" is added to group "sales"
   ```

7. Use **`(config-radsrv)#nas`** to add a NAS entry.

   ```
   RFS7000(config-radsrv)#nas ?
   A.B.C.D/M  Radius client IP address

   RFS7000(config-radsrv)#nas 10.10.10.0/24 ?
   key  Radius client shared secret

   RFS7000(config-radsrv)#nas 10.10.10.0/24 key ?
   0     Password is specified UNENCRYPTED
   2     Password is encrypted with password-encryption secret
   LINE  The secret(client shared secret), upto 32 characters
   RFS7000(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
   ```

8. Use **(config-radsrv)#proxy** to add a realm name.

   ```
   RFS7000(config-radsrv)#proxy realm mydomain.com server 10.10.1.10 port 1812
   secret 0 testing
   ```

9. Save the changes and restart the RADIUS service.

   ```
   RFS7000(config-radsrv)#service radius restart
   Sep 08 17:48:04 2006: %PM-5-PROCSTOP: Process "radiusd" has been stopped
   Sep 08 17:48:05 2006: RADCONF: radius config files generated successfully
   RFS7000(config-radsrv)#Sep 08 17:48:05 2006: %DAEMON-6-INFO: radiusd[8830]: Ready
   to process requests.
   ```

13.1.8 help

▶ *RADIUS Configuration Commands*

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-radsrv)#help?
  help  Description of the interactive help system

RFS7000(config-radsrv)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-radsrv)#
```

13.1.9 ldap-server

▶ RADIUS Configuration Commands

Use this command to configure LDAP server parameters. It uses the exisitng external database in form of active directory with the onboard RADIUS server instead of loacl database on the switch.

Syntax

```
ldap-server[primary|secondary] (host <A.B.C.D>) (port <1-65535>)
(login <name>) (bind-dn <name>) (base-dn <name>) (passwd [0|2|WORD]) (passwd-
attr0 (group-attr)(group-filter)(group-membership)(net-timeout)
```

Parameters

primary	Primary LDAP server configuration.
secondary	Secondary LDAP server configuration.
host <LDAP IP Address>	LDAP server ip configuration. • A.B.C.D – LDAP server ip address
port <number>	Enter the TCP/IP port number for the LDAP server acting as the data source.
login	Use the following as the login: `(sAMAccountName=%{Stripped-User-Name:-%{User-Name}})`
bind-dn	Specifies the distinguished name to bind with the LDAP server.
base-dn	Specifies a distinguished name that establishes the base object for the search. The base object is the point in the LDAP tree at which to start searching.
passwd	Enter a valid password for the LDAP server.
passwd-attr	Enter the password attribute used by the LDAP server for authentication.
group-attr	Specifies the group attribute used by the LDAP server.
group-filter	Specifies the group filters used by your LDAP server.
group-membership	Specifies the Group Member Attribute sent to the LDAP server when authenticating users.
net-timeout	Enter a timeout the system uses to terminate the connection to the RADIUS Server if no activity is detected.

Usage Guidelines

Use the login filter and group filter values, described in the example below, for all LDAP configuration scenarios.

Use `passwd` parameter to enter the password for active directory user mentioned in bind -dn. This will be used for initial login to the active directory.

The `passwd-attr` and `group-membership` is retained as described in the example.

Example

```
RFS7000(config)#ldap-server primary host 192.192.1.88 port 389 login
(sAMAccountName=%{Stripped-User-Name:-%{User-Name}}) bin
d-dn cn=admin,ou=wid,dc=symbolTech,dc=local base-dn ou=wid,dc=symbolTech,dc=local
passwd SYMBOL@123 passwd-attr UserPassword
group-attr cn group-filter (|(&(objectClass=group)(member=%{Ldap-
UserDn}))(&(objectClass=GroupOfUniqueNames)(uniquemember=%{L
dap-UserDn}))) group-membership radiusGroupName net-timeout 1
RFS7000(config)#
```

13.1.10 nas

▶ *RADIUS Configuration Commands*

Use this command to configure the RADIUS client.

Syntax

```
nas(A.B.C.D/M)key(0|2|LINE)
```

Parameters

A.B.C.D/M	RADIUS Client IP address.
key	RADIUS Client shared key.
0	Password is specified UNENCRYPTED.
2	Password is encrypted with password-encryption secret.
LINE	The secret (client shared secret), up to 32 characters.

Usage Guidelines

Configure the IP address range in *network access service* (NAS) to service RADIUS access request from clients falling within the range mentioned. Only 25 NAS entries can be configured on RFS7000.

Example

```
RFS7000(config-radsrv)#nas ?
A.B.C.D/M  Radius client IP address

RFS7000(config-radsrv)#nas 10.10.10.0/24 ?
key  Radius client shared secret

RFS7000(config-radsrv)#nas 10.10.10.0/24 key ?
0     Password is specified UNENCRYPTED
2     Password is encrypted with password-encryption secret
LINE  The secret(client shared secret), upto 32 characters

RFS7000(config-radsrv)#nas 10.10.10.0/24 key 0 very-secret!!
```

13.1.11 no

▶ *RADIUS Configuration Commands*

Use this command to negate a command or set its defaults.

Syntax

```
no(authentication|ca|crl-check|group|ldap-server|nas|proxy|rad-
user|server|service)
```

Parameters

authentication	RADIUS authentication.
ca	Configures ca certificate parameters.
crl-check	Certificate Revocation List (CRL) check.
group	Local RADIUS Server group configuration.
ldap-server	LDAP server parameters.
nas	RADIUS client.
proxy	RADIUS proxy server.
rad-user	RADIUS user configuration.
server	Configures server certificate parameters.
service	Service commands.

Example

```
RFS7000(config-radsrv)#no authentication data-source
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#no ca trust-point
RFS7000(config-radsrv)#
```

13.1.12 proxy

▶ *RADIUS Configuration Commands*

Use this command to configure a proxy RADIUS server based on the realm/suffix.

Syntax

```
proxy(realm|retry-count|retry-delay)
proxy relam(WORD)server(A.B.C.D)port(<1024-65535>)secret(0|2|WORD)
```

Parameters

realm WORD	Realm name is a string of up to 50 characters. • server (A.B.C.D) – Proxy server IP address. • port <1024-65535> – Proxy server port number. • secret (0|2|WORD) – Proxy server secret string. • 0 – Password is specified UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • WORD – The proxy server shared secret upto 32 characters.
retry-count *<3-6>*	Proxy server retry count value.
retry-delay*<5-10>*	Proxy server retry delay time (in seconds).

Usage Guidelines

Only five RADIUS proxy server's can be configured. The proxy server attempts six retries before it times out. The retry count defines the number of times the switch transmits each RADIUS request to the server before giving up. The timeout value defines the duration for which the switch waits for a reply to a radius request before retransmitting the request.

Example

```
RFS7000(config-radsrv)#proxy realm Test server 10.10.10.1 port 2220 secret "Very
Very Secret !!!"
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#proxy retry-count 5
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#proxy retry-delay 8
RFS7000(config-radsrv)#
```

13.1.13 rad-user

▶ *RADIUS Configuration Commands*

Use this command to configure RADIUS user parameters.

Syntax

```
rad-user(WORD)password(0|2|WORD) (group)(guest)(expiry-time)(expiry-date)
(start-time))start-date)
```

Parameters

WORD	Enter a user name up to 64 characters in length.
password*(0|2|WORD)*	RADIUS user password. • 0 – Password is specified as UNENCRYPTED. • 2 – Password is encrypted with a password-encryption secret. • WORD – Enter password up to 21 characters in length.
group	Specifies the RADIUS server group configuration.
guest	Enables guest user access.
expiry-time	Sets the expiry time for the the guest user.
expiry-date	Sets the expiry date for the guest user.
start-time	Sets the starting time for the guest user.
start-date	Sets the starting date for the guest user.

Usage Guidelines

Use `group,guest, expiry-time expiry-date,start-time` and `start-date` parameters to create a RADIUS guest user.

The RADIUS user group specified while creating a guest user must be a *guest-group*.

Example

```
RFS7000(config-radsrv)#rad-user TestRadUser password "I SPY U"
RFS7000(config-radsrv)#

RFS7000(config-radsrv)#rad-user guest1 password 0 password1 group guest-group
guest expiry-time 12:12 expiry-date 05:12:2007 start-time 12:12 start-date
05:11:2007
RFS7000(config-radsrv)#
```

13.1.14 server

▶ *RADIUS Configuration Commands*

Use this command to configure server certificate parameters used by RADIUS server. The server certiificate is a part of trustpoint created *crypto on page 5-17*.

Syntax

```
server trust-point
```

Parameters

trust-point (WORD)	Trust point configuration. • WORD – Existing trust point name.

Usage Guidelines

Create a trustpoint using `(crypto-pki-trustpoint)`. Server certificate must be created under the trustpoint using the crypto-pki commands. Refer to *crypto on page 5-17* for more details.

Example

```
RFS7000(config-radsrv)#server trust-point TestTP
RFS7000(config-radsrv)#
```

13.1.15 service

▶ RADIUS Configuration Commands

Use this command to invoke service commands to trobuleshoot or debug (config-radsrv) instance configurations. This command is also used to enable the RADIUS Server.

Syntax

```
service (show) (cli)
```

Parameters

show (cli)	Shows running system information.

Example

```
RFS7000(config-radsrv)#service show cli
Radius Configuration mode:
+-authentication
  +-data-source
    +-ldap [authentication data-source (local|ldap)]
    +-local [authentication data-source (local|ldap)]
  +-eap-auth-type
    +-all [authentication eap-auth-type (ttls-md5|ttls-pap|ttls-mschapv2|peap-
gtc|peap-mschapv2|tls|all)]
    +-peap-gtc [authentication eap-auth-type (ttls-md5|ttls-pap|ttls-
mschapv2|peap-gtc|peap-mschapv2|tls|all)]
    +-peap-mschapv2 [authentication eap-auth-type (ttls-md5|ttls-pap|ttls-
mschapv2|peap-gtc|peap-mschapv2|tls|all)]
    +-tls [authentication eap-auth-type (ttls-md5|ttls-pap|ttls-mschapv2|peap-
gtc|peap-mschapv2|tls|all)]
    +-ttls-md5 [authentication eap-auth-type (ttls-md5|ttls-pap|ttls-
mschapv2|peap-gtc|peap-mschapv2|tls|all)]
    +-ttls-mschapv2 [authentication eap-auth-type (ttls-md5|ttls-pap|ttls-
mschapv2|peap-gtc|peap-mschapv2|tls|all)]
    +-ttls-pap [authentication eap-auth-type (ttls-md5|ttls-pap|ttls-
mschapv2|peap-gtc|peap-mschapv2|tls|all)]
+-ca
  +-trust-point
    +-WORD [ca trust-point WORD]
+-clrscr [clrscr]
+-crl-check
  +-enable [crl-check enable]
+-do
  +-LINE [do LINE]
+-end [end]
+-exit [exit]
+-group
  +-WORD [group WORD]
+-help [help]
+-ldap-server
  +-primary
    +-host
      +-A.B.C.D
        +-port
          +-<1-65535>
            +-login
              +-WORD
                +-bind-dn
..................................................................................
..................................................................................
RFS7000(config-radsrv)#
```

13.1.16 show

▶ *RADIUS Configuration Commands*

Use this command to view current system information.

Syntax

```
show<paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Usage Guidelines

To view the show command parameters of RADIUS, refer to *radius on page 2-51*.

Example

```
RFS7000(config-radsrv)#show ?
  access-list           Internet Protocol (IP)
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                crypto
  debugging             Display debugging setting
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status and configuration
  ip                    Internet Protocol (IP)
  ldap                  ldap server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   Media Access Control
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  radius                Radius configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Display debug info for ACL, VPN and NAT
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  startup-config        Contents of startup configuration
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands

RFS7000(config-radsrv)#show
```

```
RFS7000(config)#show radius trust-point

Trust-point Configured For Radius
________________________________
        Server Trust-point : tp1
        CA Trust-point     : default-trustpoint



RFS7000(config)#show radius configuration

Radius Server Configuration
---------------------------
         Server Status : enabled
         Data Source   : local

RFS7000(config)#
```

14

Wireless Instance

Use the **`(config-wireless)`**instance to configure wireless parameters.

14.1 Wireless Configuration Commands

Table 14.1 summarizes the Global Config commands.

Table 14.1 Wireless Configuration Command Summary

Command	***Description***	***Ref.***
adopt-unconf-radio	Adopts a radio even if not configured. The default templates is used for configuration.	page 14-3
adoption-pref-id	Defines spreference identifier for the switch. All radios configured with this preference identifier are more likely to be adopted by this switch.	page 14-4
ap-detection	Access port detection configuration commands.	page 14-5
broadcast-tx-speed	Sets the rate at which broadcast and multicast traffic must be transmitted.	page 14-6
clrscr	Clears the display screen.	page 14-7
convert-ap	Changes the mode of operation of an access port.	page 14-8
country-code	Configures the country of operation. Regulatory configuration (channels, self healing offset) of all configured radios is reset to default values.	page 14-9

Command	**Description**	**Ref.**
dhcp-sniff-state	Record mobile unit DHCP state information.	page 14-10
dot11-shared-key-auth	Enables support for 802.11 shared key authentication.	page 14-11
end	Ends the current mode and moves to the EXEC mode.	page 14-12
exit	Ends the current mode and moves to the previous mode.	page 14-13
fix-windows-dhcp	Converts Windows DHCP Server responses to `Unicast` instead of `Broadcast`.	page 14-14
help	Describes the interactive help system.	page 14-15
ids	Intrusion detection configuration commands.	page 14-16
mac-auth-local	Local MAC authentication list.	page 14-18
manual-wlan-mapping	Allows manual mapping/un-mapping of WLANs to configured radios.	page 14-19
mobile-unit	Configures mobile unit related parameters.	page 14-20
mobility	Configures mobility parameters.	page 14-21
multicast-packet-limit	Sets a multicast packet limit per second for VLAN.	page 14-22
no	Negates a command or set its defaults.	page 14-23
oversized-frames	Attempts to use oversized frames for data traffic.	page 14-24
proxy-arp	Responds to ARP requests on behalf of mobile units.	page 14-25
qos-mapping	QoS mappings between the wired and wireless domains.	page 14-26
radio	Radio related commands.	page 14-27
self-heal	Self healing configuration commands.	page 14-33
sensor	*Wireless Intrusion Protection System* (WIPS) parameters.	page 14-35
service	Service commands.	page 14-36
show	Shows running system information.	page 14-38
smart-scan-channels	Specifies a list of channels used on the network. This list is provided to mobile units that support partial scanning.	page 14-40
wlan	Wireless LAN related commands.	page 14-41

14.1.1 adopt-unconf-radio

▶ *Wireless Configuration Commands*

Use this command to adopt a radio (even if not yet configured). The default templates is used for configuration.

Syntax

```
adopt-unconf-radio
```

Parameters

enable	Enables the adoption of unconfigured radios.

Example

```
RFS7000(config-wireless)#adopt-unconf-radio enable
RFS7000(config-wireless)#
```

14.1.2 adoption-pref-id

▶ *Wireless Configuration Commands*

Use this command as a preference identifier for the switch. Radios configured with this preference identifier are more likely to be adopted by this switch.

Syntax

```
adoption-pref-id
```

Parameters

<1-65535>	Select a pref-ID within 1-65535.

Example

```
RFS7000(config-wireless)#adoption-pref-id 500
RFS7000(config-wireless)#
```

14.1.3 ap-detection

▶ *Wireless Configuration Commands*

Use this command to configure access port detection.

Syntax

```
ap-detection
[approved|enable|mu-assisted-scan|timeout (approved|unapproved)]

ap-detection approved add <1-200> (MAC Address)(SSID)
ap-detection mu-assisted-scan(enable|refresh<10-86400>)
```

Parameters

approved	The approved access port list. • add *<1-200>* – Adds an entry to the approved access port list. • MAC Address – Select either: • MAC– MAC address in AA-BB-CC-DD-EE-FF format. • any– Any MAC address. • SSID – Select either: • LINE–A string of up to 32 characters. • any– Any SSID.
enable	Allows access ports to look for access points.
mu-assisted-scan	Mobile unit assisted scanning. • enable – Enable mobile unit assisted scanning. • refresh*<300-86400>* – The period in seconds with which all scan-capable mobile units are requested to scan for neighboring access port's.
timeout *<1-65535>*	The interval (in seconds) an access port remains in the list after it is no longer seen. Select one of the following options for timeout implementation. • approved • unapproved

Example

```
RFS7000(config-wireless)#ap-detection enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-detection approved add 150 any any
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-detection mu-assisted-scan enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-detection mu-assisted-scan refresh 520
RFS7000(config-wireless)#

RFS7000(config-wireless)#ap-detection timeout 500
RFS7000(config-wireless)#
```

14.1.4 broadcast-tx-speed

▶ *Wireless Configuration Commands*

Use this command to configure the rate broadcast and multicast traffic must be transmitted between the switch and mobile units.

Syntax

```
broadcast-tx-speed(range|throughput)
```

Parameters

range	Uses the lowest basic rate. Provides maximum range.
throughput	Uses thhighest be asic rate. Provides maximum throughput (default).

Example

```
RFS7000(config-wireless)#broadcast-tx-speed range
RFS7000(config-wireless)#

RFS7000(config-wireless)#broadcast-tx-speed throughput
RFS7000(config-wireless)#
```

14.1.5 clrscr

▶ *Wireless Configuration Commands*

Use this command to clear the screen.

Syntax

```
clrscr
```

Parameters

None.

Example

```
RFS7000(config-wireless)#clrscr
RFS7000(config-wireless)#
```

14.1.6 convert-ap

▶ *Wireless Configuration Commands*

Use this command to change an access port’s mode of operation to either sensor or standalone.

Syntax

```
convert-ap <1-256>(default|sensor)
```

Parameters

<1-256>	Indices of the access port’s to be converted (from the ['show wireless ap' command]).
default	Does not force conversion. Lets the access port negotiate its normal mode of operation with the switch.
sensor	Converts an AP300 to operate as an IDS sensor. **NOTE** The switch does not adopt this access port again until it is converted back to a regular AP300 using the [sensor MAC revert-to-ap] command.

Example

```
RFS7000(config-wireless)#convert-ap 1 default
RFS7000(config-wireless)#
```

14.1.7 country-code

▶ *Wireless Configuration Commands*

Use this command to configure the country of operation. This command erases the radio's existing configuration.

Syntax

```
country-code <country-code>
```

Parameters

country-code	Uses the two letter ISO-3166 country code ("show wireless country-code-list") to view the list of supported countries.

Usage Guidelines

Use show wireless country code to view the list of supported countries.

Example

```
RFS7000(config)#country-code us
WARNING: Select only the country in which you are using the device.
Any other selection may make the operation of this device illegal.
RFS7000(config)#
```

14.1.8 dhcp-sniff-state

▶ *Wireless Configuration Commands*

Use this command to record mobile unit DHCP state information.

Syntax

```
dhcp-sniff-state
```

Parameters

enable	Enables the recording of DHCP state information for mobile units.

Example

```
RFS7000(config-wireless)#dhcp-sniff-state enable
RFS7000(config-wireless)#
```

14.1.9 dot11-shared-key-auth

▸ *Wireless Configuration Commands*

Use this command to enable support for 802.11 shared key authentication.

NOTE Shared key authentication has known weaknesses that can compromise your WEP key. It must only be configured to accomodate wireless stations unable to conduct Open System authentication.

Syntax

```
dot11-shared-key-auth
```

Parameters

enable	Enables support for shared key authentication.

Example

```
RFS7000(config-wireless)#dot11-shared-key-auth enable
RFS7000(config-wireless)#
```

14.1.10 end

▶ *Wireless Configuration Commands*

Use this command to end and exit from the current mode and change to the PRIV EXEC mode. The prompt changes to `RFS7000#`.

Syntax

```
end
```

Parameters

None.

Example

```
RFS7000(config-wireless)#end
RFS7000#
```

14.1.11 exit

▶ *Wireless Configuration Commands*

Use this command to exit the current mode and move to the previous mode `(config)`. The prompt changes to `RFS7000(config)#`.

Syntax

```
exit
```

Parameters

None.

Example

```
RFS7000(config-wireless)#exit
RFS7000(config)#
```

14.1.12 fix-windows-dhcp

▶ *Wireless Configuration Commands*

Use this command to convert Windows DHCP Server responses to unicast instead of broadcast.

Syntax

```
fix-windows-dhcp
```

Parameters

enable	Enables support for converting Windows DHCP Server responses.

Example

```
RFS7000(config-wireless)#fix-windows-dhcp enable
RFS7000(config-wireless)#
```

14.1.13 help

▸ *Wireless Configuration Commands*

Use this command to access the system's interactive help system.

Syntax

```
help
```

Parameters

None.

Example

```
RFS7000(config-wireless)#help
CLI provides advanced help feature.  When you need help,
anytime at the command line please press '?'.

If nothing matches, the help list will be empty and you must backup
until entering a '?' shows the available options.
Two styles of help are provided:
1. Full help is available when you are ready to enter a
   command argument (e.g. 'show ?') and describes each possible
   argument.
2. Partial help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input
   (e.g. 'show ve?'.)

RFS7000(config-wireless)#
```

14.1.14 ids

▶ *Wireless Configuration Commands*

Use this command to configure Intrusion Detection System settings.

Syntax

```
ids(anomaly-detection|detect-window|ex-ops)

ids anomaly-detection(all|invalid-frame-length|multicast-source|
null-destination|same-source-destination|tkip-countermeasures|weak-wep-iv)
(enable|filter-ageout)

ids detect-window<5-300>

ids ex-ops(80211-replay-fails|all|association-requests|
authentication-fails|crypto-replay-fails|decryption-fails|
disassociations|eap-starts|probe-requests|unassoc-frames)
(filter-ageout<0-86400>|threshold(mu|radio|switch)<0-9999>)
```

Parameters

anomaly-detection	Configures parameters related to the detection of anomalous frames on the RF network. • all – Enables anomalous frames. • invalid-frame-length – Invalid frame lengths. • multicast-source – Broadcast or multicast source. • null-destination – All zero's addess. • same-source-destination – Identical source and destination addresses. • tkip-countermeasures – Filters mobile units that cause tkip countermeasures. • weak-wep-iv – Uses weak wep sequence numbers. • enable – Enables monitoring and filtering. • filter-ageout – Sets the number of seconds mobile units must be filtered.
detect-window*<5-300>*	Sets the number of seconds information must be collected before analysis. All the thresholds are a function of this window size.

ex-ops	Configures parameters related to the detection of excessive operations on the RF network. • 80211-replay-fails – 802.11 replay check failure. • all – Changes for all types of excessive operations. • association-requests – 802.11 Authentication and Association Requests. • authentication-fails – Failure to Authenticate with Servers (Radius/Kerberos). • crypto-replay-fails – TKIP/CCMP IV replay check failure. • decryption-fails – Decryption failures. • disassociations – Disassociation and de-authentication frames. • eap-starts – EAP (802.1x) start frames. • probe-requests – Probe request frames. • unassoc-frames – Frames from unassociated station. • filter-ageout<0-86400> – Configures number of seconds mobile units must be filtered out. • *threshold* (*mu*|*radio*|*switch*) <*0-9999*> – Configures the threshold of events allowed in the detection window. • mu–Uses the threshold value for monitoring on a per-mobile unit basis. • radio–Uses the threshold value for monitoring on a per-radio basis. • switch–Uses the threshold value for monitoring at the switch level.

Example

```
RFS7000(config-wireless)#ids anomaly-detection tkip-countermeasures enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#ids detect-window 250
RFS7000(config-wireless)#

RFS7000(config-wireless)#ids ex-ops 80211-replay-fails filter-ageout 5200
RFS7000(config-wireless)#
```

14.1.15 mac-auth-local

▶ *Wireless Configuration Commands*

Use this command to configure local MAC authentication list.

Syntax

```
mac-auth-local<1-1000> (allow|deny)(Starting MAC Address)(Ending MAC
Address)(range/list of WLAN indicies)WORD
```

Parameters

<1-1000>	Entry for `mac-auth-local`.
allow	Allows mobile units that match this rule to associate.
deny	Denies association to mobile units that match this rule.
Starting MAC Address	Starting MAC address in `AA-BB-CC-DD-EE-FF` format.
Ending MAC Address	Ending MAC address in `AA-BB-CC-DD-EE-FF` format.
Range/List of WLAN Indices	A list (eg: 1,3,7) or range (eg: 3-7) of WLAN indices.
WORD	Optional radio description substring.

Example

```
RFS7000(config-wireless)#mac-auth-local 452 allow 12.11.11.120 12.11.11.150 3-7
TestString
RFS7000(config-wireless)#
```

14.1.16 manual-wlan-mapping

▶ *Wireless Configuration Commands*

Use this command to manually map/un-map WLANs configured on a radio.

Syntax

```
manual-wlan-mapping
```

Parameters

enable	Enables support for manual WLAN mapping.

Example

```
RFS7000(config-wireless)#manual-wlan-mapping enable
RFS7000(config-wireless)#
```

14.1.17 mobile-unit

Wireless Configuration Commands

Use this command to configure mobile unit related parameters.

Syntax

```
mobile-unit (association-history(enable)|probe-history)
mobile-unit probe-history (add<1-200> <MAC Address>|enable)
```

Parameters

association-history	Enables the mobile unit's association history. • enable – Enables the mobile unit's association history.
probe-history	Mobile unit probe logging configuration commands. • add <1-200> – Adds a mobile unit to probe history logging. Select an index value between 1 to 200, to add probe logging MAC. • MAC Address – The MAC address of the mobile used for probe history logging.
enable	Enables mobile unit probe logging.

Example

```
RFS7000(config-wireless)#mobile-unit probe-history enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobile-unit association-history enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobile-unit probe-history add 20 AA-BB-CC-DD-EE-FF
RFS7000(config-wireless)#
```

14.1.18 mobility

▶ *Wireless Configuration Commands*

Use this command to configure mobility parameters

Syntax

```
mobility(enable|local-address|max-roam-period|peer)
mobility local-address (IP Address)
mobility max-roam-period<1-300>
mobililty peer (IP Address)
```

Parameters

enable	Enables mobility globally.
local-address	Sets the local address for mobility. • A.B.C.D – IP Address of A.B.C.D format.
max-roam-period *<1-300>*	Sets the maximum roam period for a mobile unit (in seconds).
peer	Adds a peer to this mobility region. • A.B.C.D – IP address of the Peer.

Example

```
RFS7000(config-wireless)#mobility enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobility local-address 12.12.12.1
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobility max-roam-period 10
RFS7000(config-wireless)#

RFS7000(config-wireless)#mobility peer 157.208.235.108
RFS7000(config-wireless)#
```

14.1.19 multicast-packet-limit

▶ *Wireless Configuration Commands*

Use this command to a configure multicast packet limit per second for VLAN.

Syntax

```
multicast-packet-limit <0-128> (<1-4094>|<vlan range>)
```

Parameters

<0-128>	Multicast packet limit per second.
<1-4094>	Single VLAN ID (1-4094) that the new limit applies to.
<vlan range>	A list (1,3,7) or range (3-7) of VLAN IDs.

Example

```
RFS7000(config-wireless)#multicast-packet-limit 120 50
RFS7000(config-wireless)#multicast-packet-limit

RFS7000(config-wireless)#multicast-packet-limit 120 1,10,25 RFS7000(config-
wireless)#multicast-packet-limit
```

14.1.20 no

▶ *Wireless Configuration Commands*

Use this command to negate a command or set its defaults.

Syntax

```
no(adopt-unconf-radio|adoption-pref-id|ap-detection|broadcast-tx-speed|country-
code|dhcp-sniff-state|dot11-shared-key-auth|fix-windows-dhcp|ids|mac-auth-
local|manual-wlan-mapping|mobile-unit|mobility|oversized-frames|proxy-arp|qos-
mapping|radio|self-heal|sensor|service|smart-scan-channels|wlan)
```

Parameters

Refer to *Table 14.1 on page 14-1* for the parameters negated using the **no** command.

Example

```
RFS7000(config-wireless)#no mobility enable
RFS7000(config-wireless)#
```

14.1.21 oversized-frames

▶ *Wireless Configuration Commands*

Use this command to use oversized frames for data traffic.

Syntax

```
oversized-frames
```

Parameters

enable	Enables support for oversized frames.

Example

```
RFS7000(config-wireless)#oversized-frames enable
RFS7000(config-wireless)#
```

14.1.22 proxy-arp

▶ *Wireless Configuration Commands*

Use this command to respond to ARP requests on behalf of mobile units.

Syntax

```
proxy-arp
```

Parameters

enable	Enables support for proxy arp.

Example

```
RFS7000(config-wireless)#proxy-arp enable
RFS7000(config-wireless)#
```

14.1.23 qos-mapping

▶ *Wireless Configuration Commands*

Use this command to configure QoS mappings between wired and wireless domains.

Syntax

```
qos-mapping(wired-to-wireless|wireless-to-wired)

qos-mapping wired-to-wireless(dot1p<0-7>|dscp<0-63>)
(background|best-effort|video|voice)

qos-mapping wireless-to-wired(background|best-effort|video|voice)
dot1p<0-7>
```

Parameters

wired-to-wireless	Mappings used while switching wired traffic over the air. • dot1p<*0-7*> – Configures the mapping of 802.1p tags to access categories. Specify more than one 802.1p tag (0-7) to configure. • dscp<*0-63*> – Configures the mapping of DSCP values to access categories. Specify more than one DSCP value (0-63) to configured. • background – Background category traffic. • best-effort – Best effort category traffic. • video – Video traffic category traffic. • voice – Voice traffic category traffic.
wireless-to-wired	Mappings used while switching wireless traffic to rest of network. • dot1p<*0-7*> – Configures the 802.1p tags that corresponds to selected access category.

Example

```
RFS7000(config-wireless)#qos-mapping wireless-to-wired background dot1p 5
RFS7000(config-wireless)#
```

14.1.24 radio

▶ *Wireless Configuration Commands*

Use this command to configure radio related settings.

Syntax

```
radio (<1-4096>|RADIO|add|all-11a|all-11b|all-11bg|
configure-8021X|default-11a|default-11b|default-11bg|dns-name)

radio<1-4096>(adoption-pref-id|antenna-mode|beacon-interval|bss|
cca-level|cca-mode|channel-power|coordinates|
copy-config-from|description|detector|dtim-period|enforce-spec-mgmt|
location-message|mac|max-mobile-units|mu-power <0-20>|
on-channel-scan|reset|reset-ap|rts-threshold|run-acs|
self-heal-offset|short-preamble|speed|wmm)

radio <1-4096> bss(<1-4>|auto>)WLAN
radio <1-4096> channel-power(indoor|outdoor)(<1-200>|acs|random)<4-20>
radio <1-4096> coordinates (x coordinates) (y coordinates)(z coordinates)
radio <1-4096> copy-config-from(<1-1000>|default-11a|default-11b|default-11bg)
radio <1-4096> dtim-period<1-50> bss<1-4>

radio range(1|11|12|18|2|24|36|48|54|5p5|6|9|basic1|basic11basic12|
basic18|basic2|basic24|basic36|basic48|basic54|basic5p5|basic6|basic9|
default|range|throughput)

radio wmm(background|best-effort|video|voice)(aifsn<1-15>|burst<0-65535>|
cw<0-15>)

radio add<1-4096>(MAC Address)(11a(ap300)|11b(ap100|ap4131)|11bg(ap300))
```

Parameters

<1-4096>	A single radio index.
default-11bg	default 11bg configuration template.
adoption-pref-id *<0-65535>*	A preference identifier for this radio. The radio is more likely to be adopted by a preferred switch. **NOTE** An AP300 has two radio's. Configuring any one radio as a pref-id ensures the other radio is also configured with this pref-id. An AP300 cannot be adopted by two switches simultaneously.
antenna-mode *<diversity|primary|secondary>*	Antenna diversity mode. Select from the following options: • diversity–Full diversity (both antennas). • primary–Primary antenna only. • secondary–Secondary antenna only. **NOTE** Before executing this command, ensure the radio is present and is an AP300.
beacon-interval*<50-200>*	Beacon interval in K-uSec.

bss (<*1-4*>|auto) WLAN	Map wireless LANs to radio BSSID's. - <1-4> –The BSS where a wireless ILAN is mapped. - auto – Automatic assignment of BSS. If the user selects wireless lans d the system assigns them to a BSS automatically. - WLAN – A list (1,3,7) or range (3-7) of WLAN indices. When a BSS is specified, the first WLAN is used as the primary WLAN. When the auto option is used, the system automatically assigns the first four WLANs as primaries on their respective BSS's.
cca-level<*1-31*>	CCA level value.
cca-mode<*0-3*>	CCA mode value.
channel-power (indoor|outdoor) (<1-2000>|acs|random) <4-20>	Location, channel and transmit power level. - indoor – Indoor location. - outdoor – Outdoor location. - <1-2000> – Channel number. - acs – Auto channel selection (radio scans for the least congested channel at startup or reconfiguration). - random – Random channel selection. - <4-20> – Power in dBm.
coordinates (X,Y,Z coordinates)	Configures the location of this radio using x.y.z coordinates. - <-65535-65535> – X Coordinate. - <-65535-65535> – Y Coordinate. - <-65535-65535> – Z Coordinate.
copy-config-from (<1- 4096>|default-11a| default-11b|default-11bg)	Copies the configuration from a previously configured radio. - <1- 4096> – A single radio index. - default-11a – default 11a configuration template. - default-11b – default 11b configuration template. - default-11bg – default 11bg configuration template.
description	Configures a description for this radio. Must not exceed 20 characters.
detector	Dedicates this radio as a detector. No mobile units can associate to a detector.
dtim-period<*1-50*> bss <*1-4*>	DTIM period (number of beacons between successive DTIMs) - <*1-50*> – DTIM period. - bss – *BSS.* - <1-4> – BSS index.
enforce-spec-mgmt (enable)	Enforces spectrum management checks on specified radios. Only mobile units that advertise spectrum management are allowed to associate to this radio.
location-message	Specifies a message sent to mobile units that associate with these radios. This message must not exceed 80 characters.

mac (AA-BB-CC-DD-EE-FF)	Changes the parent (access port) MAC address of the radio. • AA-BB-CC-DD-EE-FF – MAC address in AA-BB-CC-DD-EE-FF format.
max-mobile-units *<1-256>*	Maximum number of mobile units allowed to associate.
mu-power <0-20>	Power adjustment level for mobile units associated with this access port. Mobile units that support this element must reduce their transmit power by the specified value. • <0-20> – Power in dBm.
on-channel-scan	Enables rogue scanning on this radio.
reset	Resets a radio (this only resets the specified radio, not the complete access port).
reset-ap	Resets the parent access port (this resets all radios on that access port).
rts-threshold*<0-2347>*	RTS threshold in bytes.
run-acs	Runs Auto Channel Selection on a radio. The radio must already have been configured for ACS.
self-heal-offset *<0-30>*	Configures the self healing offset, measured in dBm, for regulatory. **Note** This offset is based off the regulatory maximum power for the specified channel (the command "show wireless regulatory" shows the max power allowed).
short-preamble	Enables short preamble support. **Note** This disables support for long preamble, mobile units that only support long preamble will not be able to associate.

speed	Configures the basic and supported data rates. • 1 1-Mbps. • 11 11-Mbps. • 12 12-Mbps. • 18 18-Mbps. • 2 2-Mbps. • 24 24-Mbps. • 36 36-Mbps. • 48 48-Mbps. • 54 54-Mbps. • 5p5 5.5-Mbps. • 6 6-Mbps. • 9 9-Mbps. • basic1 basic 1-Mbps. • basic11 basic 11-Mbps. • basic12 basic 12-Mbps. • basic18 basic 18-Mbps. • basic2 basic 2-Mbps. • basic24 basic 24-Mbps. • basic36 basic 36-Mbps. • basic48 basic 48-Mbps. • basic54 basic 54-Mbps. • basic5p5 basic 5.5-Mbps. • basic6 basic 6-Mbps. • basic9 basic 9-Mbps. • default Factory default rates based on radio type. • range All rates enabled, the lowest one set to basic. • throughput All rates basic (note: only g clients allowed on 11bg radios).

wmm (background|best-effort|video|voice) (aifsn<*1-15*>|burst<*0-65535*>| cw<*0-15*>)	802.11e / Wireless MultiMedia (WMM) parameters (supported only on AP300). • background – Background category traffic. • best-effort– Best effort category traffic. • video –Video traffic category traffic. • voice – Voice traffic category traffic. • aifsn<*1-15*> – (Arbitration Inter Frame Spacing Number) The wait time in milliSeconds between data frames is derived using AIFSN and the slot-time. • burst<*0-65535*> – (transmit-opportunity) An interval when a particular WMM mobile unit has the right to initiate transmissions on the wireless medium. • cw<*0-15*>– (Contention Window parameters) Select a number between 0 and the minimum contention window to wait before re-attempting a transmission. MUs then double their wait time on a collision, until it reaches the maximum contention window.
RADIO	A list (3,7) or range (3-7) of radio indices.
add <*1-1000*> (MAC Address) [11a|11b|11bg] (ap300))	Adds a new radio. • <1-1000> – Index where this radio is added. • MAC – MAC address in AA-BB-CC-DD-EE-FF format. • 11a – 802.11a type radio. • 11b – 802.11b type radio. • 11bg – 802.11bg type radio. • ap300 – ap300 type access port (default for 11a and 11bg).
all-11a	All 11a radios currently in configuration.
all-11b	All 11b radios currently in configuration.
all-11bg	All 11bg radios currently in configuration.
configure-8021X	Configures the 802.1X username and password on adopted access ports.
default-11a	Default 11a configuration template.
default-11b	Default 11b configuration template.
dns-name WORD (MAC Address)	Configures the DNS name used in the L3 Discovery of adopted access ports. • AA-BB-CC-DD-EE-FF – Changes the DNS name on only the access port with the specified MAC address. If not specified, the DNS name update is sent to all adopted access ports.

Example

```
RFS7000(config-wireless)#radio 250 bss auto 3-5
RFS7000(config-wireless)#

RFS7000(config-wireless)#radio 1 channel-power indoor 1 16
Regulatory parameter values depend on country of operation and radio type.
 Refer to documentation for more regulatory information
RFS7000(config-wireless)#

RFS7000(config-wireless)#radio 1 antenna-mode diversity
RFS7000(config-wireless)#
```

14.1.25 self-heal

▶ *Wireless Configuration Commands*

Use this command to configure self healing.

Syntax

```
self-heal(interference-avoidance|neighbor-recovery)

self-heal interference-avoidance(enable|hold-time<0-65535>|
retries<0.0-15.0>)

self-heal neighbor-recovery(action|enable|neighbors|run-neighbor-detect)
self-heal neighbor-recovery action(both|none|open-rates|raise-power)
radio(<1-4096>|RADIO)
self-heal neighbor-recovery neighbors<1-1000>(<1-1000>|RADIO)
```

Parameters

interference-avoidance	Interference avoidance configuration.
enable	Enables/disables interference avoidance.
hold-time*<0-65535>*	The interval (in seconds) to disable interference avoidance after a detection . This prevents a radio from changing channels continuously. Set the hold-time between 0-65535 seconds.
retries*<0.0-15.0>*	The average number retries to force a radio to re-run auto channel selection. Set a value between 0-15.
neighbor-recovery	Neighbor recovery configuration commands.
action (both|none|open-rates| raise-power) radio (*<1- 4096>*|RADIO)	Radio self healing action when neighbors are detected down. • both – Raises the power to max and open all rates. • none – Does nothing. • open-rates – Opens all rates. • raise-power – Raises the power to max. • **radio** – Modifies the action for specified radio(s). • *<1-4096>* – A single radio index. • RADIO – A list (1,3,7) or range (3-7) of radio indices.
enable	Monitors access ports and attempts to increase coverage on failure.
neighbors*<1-1000>* (<1- 4096>|RADIO)	Adds radios as neighbors.
run-neighbor-detect	Disassociates mobile units, clears current neighbors and runs neighbor detection.

Example

```
RFS7000(config-wireless)#self-heal interference-avoidance enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#self-heal interference-avoidance hold-time 600
RFS7000(config-wireless)#

RFS7000(config-wireless)#self-heal neighbor-recovery enable
Note: reducing the configured transmit power of radios will ensure
that there is room to increase power when a neighbor fails
RFS7000(config-wireless)#

RFS7000(config-wireless)#self-heal neighbor-recovery neighbors 1 1
RFS7000(config-wireless)#
```

14.1.26 sensor

▶ *Wireless Configuration Commands*

Use this command to configure Wireless Intrusion Protection System parameters.

Syntax

```
sensor(default-config|vlan)
sensor default-config(ip-mode|wips-server-ip)
sensor default-config ip-mode(dhcp|static(A.B.C.D/M)(A.B.C.D))
sensor default-config wips-server-ip(primary|secondary)(A.B.C.D)
```

Parameters

default-config	Default configuration sent to sensors when configured.
ip-mode	Configures the IP address mode of the sensors. • dhcp – Sensors must use DHCP to obtain an IP address. • static (A.B.C.D/M)(A.B.C.D) – Sensors must use the specific static IP address. • A.B.C.D/M – Sensor IP address and network mask. • A.B.C.D – Specifies the gateway IP address for sensors.
wips-server-ip	Specifies the IP addresses of the WIPS server. • primary (A.B.C.D) – Specifies the primary IP address of the WIPS Server. • secondary (A.B.C.D) – Specifies the secondary IP address of the WIPS Server.
vlan*<1-4094>*	Configures VLANs where sensors are to be discovered.

Example

```
RFS7000(config-wireless)#sensor vlan 268 500
RFS7000(config-wireless)#
```

14.1.27 service

▶ Wireless Configuration Commands

Use this command to invoke service commands to troubleshoot or debug the `(config-wireless)` instance configuration.

Syntax

```
service(show|wireless)
service show (cli)
service show wireless (ap(history)<accessport MAC address>

service wireless (clear-ap-log<1-256>|dump-core|dump-state|rate-scale|
request-ap-log <1-256>|save-ap-log)
```

Parameters

show	Shows running system information.
cli	Shows CLI tree of current mode.
wireless	Wireless parameters.
ap (history)	Access port serviceability parameters.Use history to access port history. The following options can be used to access ap-history: • *XX-XX-XX-XX-XX-XX* – Access port MAC.
wireless	Wireless parameters.
clear-ap-log *<1-256>*	Clears access port logs for the selected access port index. Select an access port index between 1 - 256.
dump-core	Creates a core file of the `ccsrvr` process.
dump-state	Creates a `ccsrvr.dump` file in `nvram` with internal state information.
rate-scale	Enables wireless rate scaling (default).
request-ap-log*<1-256>*	Requests an access port log for the selected access port. Select an access port index between 1 - 256.
save-ap-log	Saves debug/error logs sent by the access port.

Example

```
RFS7000(config-wireless)#service show cli | include LI
          +-LINE [ap-detection approved add <1-200> (MAC|any) (LINE|any)]
          +-any [ap-detection approved add <1-200> (MAC|any) (LINE|any)]
          +-LINE [ap-detection approved add <1-200> (MAC|any) (LINE|any)]
          +-any [ap-detection approved add <1-200> (MAC|any) (LINE|any)]
  +-LINE [do LINE]
      +-<1-200> [no ap-detection approved (<1-200>|IDX-LIST)]
      +-IDX-LIST [no ap-detection approved (<1-200>|IDX-LIST)]
            +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
            +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
          +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
            +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
            +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
          +-LINE [no wlan (<1-256>|WLAN) dot11i phrase (0|2|) LINE]
      +-LINE [radio <1-4096> description LINE].................
```

```
RFS7000(config-wireless)#service show wireless ap history
RFS7000(config-wireless)#

RFS7000(config-wireless)#service wireless clear-ap-log 20
RFS7000(config-wireless)#service

RFS7000(config-wireless)#service wireless dump-core
RFS7000(config-wireless)#

RFS7000(config-wireless)#service wireless dump-core
RFS7000(config-wireless)#

RFS7000(config-wireless)#service wireless rate-scale
RFS7000(config-wireless)#

RFS7000(config-wireless)#service wireless request-ap-log 35
RFS7000(config-wireless)#

RFS7000(config-wireless)#service wireless save-ap-log
RFS7000(config-wireless)#
```

14.1.28 show

▶ Wireless Configuration Commands

Use this command to view current system information.

Syntax

```
show<paramater>
```

Parameters

?	Displays the parameters for which information can be viewed using the show command.

Example

```
RFS7000(config-wireless)#show ?
  access-list           Internet Protocol (IP)
  aclstats              Show ACL Statistics information
  alarm-log             Display all alarms currently in the system
  autoinstall           autoinstall configuration
  banner                Display Message of the Day Login banner
  boot                  Display boot configuration.
  clock                 Display system clock
  commands              Show command lists
  crypto                encryption module
  debugging             Debugging information outputs
  dhcp                  DHCP Server Configuration
  environment           show environmental information
  file                  Display filesystem information
  ftp                   Display FTP Server configuration
  history               Display the session command history
  interfaces            Interface status
  ip                    Internet Protocol (IP)
  ldap                  LDAP server
  licenses              Show any installed licenses
  logging               Show logging configuration and buffer
  mac                   MAC access-list assignment
  mac-address-table     Display MAC address table
  management            Display L3 Managment Interface name
  mobility              Display Mobility Parameters
  ntp                   Network time protocol
  password-encryption   password encryption
  privilege             Show current privilege level
  proxy-arpdb           Display proxy-ARP entries in ARP database
  radius                RADIUS configuration commands
  redundancy-group      Display redundancy group parameters
  redundancy-history    Display state transition history of the switch.
  redundancy-members    Display redundancy group members in detail
  running-config        Current Operating configuration
  securitymgr           Securitymgr parameters
  sessions              Display current active open connections
  snmp                  Display SNMP engine parameters
  snmp-server           Display SNMP engine parameters
  spanning-tree         spanning-tree Display spanning tree information
  startup-config        Contents of startup configuration
  static-channel-group  static channel group membership
  terminal              Display terminal configuration parameters
  timezone              Display timezone
  upgrade-status        Display last image upgrade status
  users                 Display information about terminal lines
  version               Display software & hardware version
  wireless              Wireless configuration commands
  wlan-acl              wlan based acl
```

```
RFS7000(config-wireless)#show
```

```
RFS7000(config-wireless)#show wireless AP
Number of access-ports adopted   : 2
Available licenses               : 254
Redundancy enabled               : N
Redundancy mode                  : active
  #        Mac           Radios [indices]    Model-Number             Adoption-
Mode
  1  00-15-70-11-34-82    2 [ 3 4 ]        WSAP-5100-100-WW         L2 (vlan: 1)
  2  00-A0-F8-EA-4C-99    2 [ 1 2 ]        WSAP-5100-100-WW         L2 (vlan: 2)
RFS7000(config-wireless)#
```

14.1.29 smart-scan-channels

▶ *Wireless Configuration Commands*

Use this command to configure a list of channels used on the network. This list is provided to mobile units that support partial scanning.

Syntax

```
smart-scan-channels(11a|11bg)<1-200>
```

Parameters

11a	Specifies a channel list for the 5Ghz band used by 802.11a mobile units.
11bg	Specifies a channel list for the 2.4Ghz band used by 802.11bg mobile units.
<1-200>	List of channels.

Example

14.1.30 wlan

▶ Wireless Configuration Commands

Use this command to configure Wireless LAN related commands.

Syntax

```
wlan(<1-256>|WLAN)
(accounting|answer-bcast-ess|authentication-type| description
|dot11i|enable|encryption-type|hotspot|inactivity-timeout|kdc|mobility|
mu-mu-disallow|qos|radius|secure-beacon|ssid|symbol-extensions
|syslog|tunnel|vlan|wep128|wep64)

wlan <1-256> accounting(none|radius|ssyslog)
wlan <1-256> authentication-type(eap|hotspot|kerberos|mac-auth|none)

wlan <1-256> dot11i(handshake|key|key-rotation|key-rotation-interval|
opp-pmk-caching|phrase|pmk-caching|preauthentication|second-key|
tkip-cntrmeas-hold-time|wpa2-tkip)
wlan <1-256> dot11i handshake timeout<100-5000> retransmit<1-10>
wlan <1-256> key(0|2|WORD)

wlan <1-256> encryption-type(ccmp|keyguard|none|tkip|tkip-ccmp|
wep128|wep128-keyguard|wep64)

wlan <1-256> hotspot(allow-list|webpage|webpage-location)
wlan <1-256> hotspot allow-list(Rule index)(IP address)
wlan <1-256> hotspot webpage(external|internal)(failure|login|welcome)
wlan <1-256> hotspot webpage-location(advanced|external|internal)

wlan <1-256> kdc(password(0||LINE)|realm(LINE)|server(primary|secondary|timeout))
wlan <1-256> kdc server (primary|secondary|timeout)auth-port<1-65535>

wlan <1-256> qos(classification|mcast1|mcast2|prioritize-voice|svp|wmm)
wlan <1-256> qos classification(background|best-effort|video|voice|wmm)
wlan <1-256> qos wmm(8021p|background|best-effort|dscp|video|voice)
(aifsn|cw|txop-limit|acm)

wlan <1-256> radius(accounting|authentication-protocol|dscp|
dynamic-authorization|dynamic-vlan-assignment|mobile-unit|reauth|server)

wlan <1-256> radius accounting(mode|timeout)
wlan <1-256> radius accounting mode(start-interim-stop(interval)
<60-3600>|start-stop|stop-only|)
wlan <1-256> radius accounting timeout<1-60> retransmit<1-100>

wlan <1-256> radius authentication-protocol(chap|pap)


wlan <1-256> radius server(primary|secondary|timeout)
wlan <1-256> radius server(primary|secondary)
(ip-address(auth-port)<1024-65535>)(radius-key(0|2|LINE))
wlan <1-256> radius server timeout<1-60> retransmit<1-10>

wlan <1-256> syslog (accounting) server<IP Address> port<Port Number>

wlan <1-256> tunnel<1-32> gateway<IP Address and mask>

wlan <1-256> wep128(key<1-4> (ascii|hex[0|2|WORD])|phrase(LINE)|
wep-default-key<1-4>)
```

Parameters

[<1-256> | WLAN]	Select a single WLAN index. You also have the option of selecting a list (1,3,7) or range (3-7) of WLAN indices.
accounting (none|radius|syslog)	Accounting on this WLAN. • none – No accounting on this WLAN. • radius – Uses RADIUS accounting on this WLAN. • syslog – Uses syslog accounting on this WLAN.
answer-bcast-ess	Allows this WLAN to respond to probes for broadcast ESS.
authentication-type (eap|hotspot|kerberos| mac-auth|none)	The authentication type of this WLAN. • eap – EAP authentication (802.1X). • hotspot – Web based authentication. • kerberos – Kerberos authentication (encryption type changes to wep128 if its not already wep128/keyguard). • mac-auth – MAC authentication (RADIUS lookup of MAC address). • none – None / pre-shared keys.
description	The description of this WLAN.

dot11i [handshake | key | key-rotation | key-rotation-interval | opp-pmk-caching | phrase|pmk-caching | preauthentication | second-key| tkip-cntrmeas-hold-time]	Modifies tkip/ccmp (802.11i) related parameters. • handshake (timeout <100-5000>) (retransmit<1-10>) – Use a handshake to configure timeout and retransmission. • timeout*<100-5000>* – The timeout (in milliseconds) between retries. • retransmit*<1-10>* – The number of retransmission attempts. • key(0|2|WORD) – Configure the key (PMK). • 0 – Password is specified UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • WORD – The 256bit (64 hex characters) long key. • key-rotation (enable) – Controls the periodic update of the broadcast keys for all associated mobile units. • key-rotation-interval *<1800-86400>* – Configures the broadcast key rotation interval. • opp-pmk-caching – Enables the opportunistic use of cached pairwise master keys (fast roaming with eap/802.1X). • phrase(0|2|LINE) – Configures the passphrase. • 0 – Password is specified UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • LINE – A passphrase between 8 and 63 characters long. • pmk-caching – Enables the use of cached pairwise master keys (fast roaming with eap/802.1X). • preauthentication – Enables support for 802.11i pre-authentication. • second-key(enable|key|phrase) (0|2|WORD) – Configures a secondary set of key/passphrase for this WLAN. • enable – Enables the use of a secondary key/passphrase. • key – Configures the key (PMK). • phrase – Configures the passphrase. • 0 – Password is specified UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • WORD – The 256bit (64 hex characters) long key. • tkip-cntrmeas-hold-time *<0-65535>* – Configures the hold-time (in seconds) that clients are blocked when tkip countermeasures are invoked. Default is 60 seconds. • wpa2-tkip (enable) – Enables support for WPA2-TKIP (in addition to WPA-TKIP) when TKIP is enabled on this WLAN.
enable()	Enables specified wireless LAN(s).

encryption-type()	The encryption type for this WLAN. • ccmp – AES Counter Mode CBC-MAC Protocol (AES-CCM/CCMP). • keyguard – Keyguard-MCM (Mobile Computing Mode). • none – No encryption. • tkip – Enables Temporal Key Integrity Protocol (TKIP). • tkip-ccmp – Enables both tkip and ccmp on this WLAN. • wep128 – Enables Wired Equivalence Privacy (WEP) with 128 bit keys. • wep128-keyguard – Enables both WEP128 as well as Keyguard-MCM on this WLAN. • wep64 – Enables Wired Equivalence Privacy (WEP) with 64 bit keys. **Note** A wep64 configuration is insecure when two WLANs are mapped to the same VLAN, and one WLAN uses no encryption and the other uses WEP.

hotspot()	Modifies hotspot related parameters. • allow (rule index) (IP address) – Modifies hotspot allow-list parameters. Users who have not yet authenticated must be allowed access to these IP addresses. • Rule index – Allow-list Rule index (must be between (1-10). • IP address – Allow-list IP address. • webpage (external|internal) (failure|login|welcome) – Modifies hotspot page parameters. • external – Modifies a hotspot's External page. • internal – Modifies hotspot's Internal page. • failure – Users are redirected to this Web page if they fail authentication. • login – Users are prompted for their username and password within this Web page. • welcome – Users are redirected to this Web page after they authenticate successfully. • webpage-location (advanced|external|internal) – The location of the Web pages used for authentication. These pages can either be hosted on the switch or an external Web Server. • advanced – Uses login/welcome/failure Web pages created by the user on the switch. • external – Uses login/welcome/failure Web pages on an external server. • internal – Use login/welcome/failure Web pages created automatically on the switch.
inactivity-timeout *<60-86400>*	Inactivity timeout in seconds. If a frame is not received from a mobile unit for this interval, the mobile unit is disassociated.

kdc [password (0||LINE) | realm (LINE) | server (primary|secondary|timeout)] auth-port*<1-65535>*	Modifies KDC related parameters. • password(0|2|LINE) – KDC server password, up to 127 characters. • 0 – Password is specified UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • LINE – KDC server password, up to 127 characters. • realm(LINE) – KDC realm, up to 127 characters. • LINE – KDC realm, up to 127 characters. • server (primary|secondary) (IP address) auth-port *<1-65535>* – Modifies KDC server parameters. • primary – Primary KDC server. • secondary – Secondary KDC server. • IP address – KDC server IP address. • auth-port*<1-65535>* – KDC server authentication port. Default is 88. • server(timeout)*<1-60>* – Modifies KDC server parameters. • timeout – Time the switch waits for a response from the KDC Server before retrying.
mobility (enable)	Enables L3 Mobility on WLAN(s).
mu-mu-disallow (switch-to-wired)	Disallows frames from one mu to another mu on this WLAN. • switch-to-wired – Disallowesd by switching the frame out on the wired side (to allow an external switch to decide whether this frame is allowed or dropped).

qos [classification | mcast1 | mcast2 | prioritize-voice | svp | wmm]	Quality of Service commands. • classification [background|best-effort|video|voice|wmm] – Select how traffic on this WLAN is classified (relative prioritization on the access port). • background – Traffic on this WLAN is treated as background traffic. • best-effort – Traffic on this WLAN is treated as best-effort. • video – Traffic on this WLAN is treated as video. • voice – Traffic on this WLAN is treated as voice. • wmm – Use WMM based classification (using DSCP or 802.1p tags) to classify traffic into different queues. • mcast1|mcast2 (AA-BB-CC-DD-EE-FF) – The Egress prioritization multicast mask. • AA-BB-CC-DD-EE-FF – MAC address in AA-BB-CC-DD-EE-FF format. • prioritize-voice – Prioritizes voice frames over general data frames (applies non-WMM mobile unit). • svp (enable) – Enables Spectralink Voice Prioritization support on this WLAN. • wmm (8021p|background| best-effort| dscp|video|voice) (aifsn|cw|txop-limit|acm) – 802.11e / Wireless MultiMedia (WMM) parameters (supported only on AP300). • 8021p – Uses 802.1p frame priority (field in the VLAN tag) to determine packet priority. • background – Background category traffic. • best-effort – Best effort category traffic. • dscp – Uses DSCP (Differentiated Services Code Point) bits in the IP header to determine packet priority. • video – Video traffic category traffic. • voice – Voice traffic category traffic.

	• aifsn – (Arbitration Inter Frame Spacing Number) The wait time (in milliSeconds) between data frames derived using AIFSN and the slot-time. • cw – (Contention Window parameters) Wireless stations pick a number between 0 and the minimum contention window to wait before retrying transmissions. Stations double their wait time on a collision, until it reaches the maximum contention window. • txop-limit – (Transmit-opportunity): An interval when a particular WMM STA has the right to initiate transmissions on the wireless medium. • acm – Admission Control Parameters.
radius [accounting | authentication-protocol | dscpdynamic-authorization | dynamic-vlan-assignment | mobile-unit | reauth | server]	Modify Radius/802.1X related parameters. • accounting mode [start-interim-stop (interval)<60-3600> | start-stop |stop-only] – Used to configure RADIUS accounting parameters. • mode – Accounting Mode on the WLAN. • start-interim-stop – Accounting Start-Interim-Stop. • interval<*60-3600*>– Interval between successive accounting updates. • start-stop – Sends Accounting Start-Stop. • stop-only – Send sAccounting Stop only. • accounting timeout<*1-60*> retransmit<*1-100*> – Configures RADIUS accounting parameters. • timeout <*1-60*>– Time in seconds the switch waits for a response from the RADIUS server before retrying accounting. • retransmit <*1-100*>– Number of retries before the switch gives up accounting. • authentication-protocol (chap|pap) – Authentication protocol to use in the radius requests. • chap – Challenge Handshake Authentication Protocol.

  - pap – Password Authentication Protocol.
- dscp<*0-63*> – Specifies a DSCP (*Differentiated Services Code Point*) v to provide QoS to RADIUS packets. The DSCP value must be between 0-63.
- dynamic-authorization (enable) – Configures support for RADIUS dynamic authorization extensions (such as Disconnect Message) and Change-Of-Authorization, as described in RFC 3576.
  - enable – Enables support for RADIUS dynamic authorization.
- dynamic-vlan-assignment – Allows users to be assigned to RADIUS Server specified VLANs, instead of the VLAN mapped to the WLAN.
  - enable – Enables dynamic/RADIUS-assigned VLAN assignment.
- mobile-unit timeout<1-60> retransmit<1-10> – Modifies RADIUS/802.1X supplicant related parameters.
  - timeout<1-60> – Time in seconds the switch waits for a response from the mobile unit before retrying.
  - retransmit<1-10> – Number of retries before the switch gives up and disassociates the mobile unit.
- reauth<*30-65535*> – Enables periodic reauthentication of all associated mobile units.
  - <*30-65535*> – Reauthentication period in seconds.
- server [primary|secondary] [ip-address (auth-port) <*1024-65535*>) radius-key (0|2|LINE)] – Modifies RADIUS/802.1X server parameters.
  - primary – Primary RADIUS server.
  - secondary – Secondary RADIUS server.
  - ip-address – RADIUS server IP address.
  - auth-port<*1024-65535*> – RADIUS server authentication port (default:1812).
  - radius-key – Radius server shared secret, upto 127 characters.
  - 0 – Password is specified UNENCRYPTED.
  - 2 – Password is encrypted with password-encryption secret.
  - LINE – Radius server shared secret, upto 127 characters.
- server timeout<1-60> retransmit<1-10> – Modify Radius/802.1X server parameters.
  - timeout<*1-60*> – Time, in seconds, the switch waits for a response from the radius server before retrying.
  - retransmit<*1-10*> – Number of retries before the switch gives up and disassociate the mobile unit.

secure-beacon	Do not include the SSID of this WLAN in Beacon frames.
ssid	The SSID of this WLAN.
symbol-extensions fast-roaming (enable)	Enables support for Symbol extensions. • fast-roaming (enable) – Enables support for Symbol fast roaming.
syslog (accounting) server <IP Address> port <Port number>	Syslog Accounting. • accounting – Modifies accounting parameters. • server <IP Address> – Modifies syslog accounting server IP address. • port <Port Number> – Syslog server port. The default port is 514.
tunnel <1-32> (gateway) <IP Address and Mask>	The tunnel index mapping for this WLAN. • <1-32> – A tunnel index. • gateway – The gateway IP address and mask. • A.B.C.D/M – IP address and mask.
vlan*<1-4094>*	The VLAN assignment of this WLAN.
wep128 (key*<1-4>* (ascii|hex)<0|2|WORD> | phrase (LINE) | wep-default-key*<1-4>)*	Configures WEP128 parameters. • key*<1-4>* – Configures pre-shared hex keys. • ascii – Keys as ascii characters (5 characters for wep64, 13 for wep128). • hex – Keys as hexadecimal characters (10 characters for wep64, 26 for wep128). • 0 – Password is specified UNENCRYPTED. • 2 – Password is encrypted with password-encryption secret. • WORD – Key (10 hex or 5 ascii characters for wep64, 26 hex or 13 ascii characters for wep128). • phrase – Specifies a passphrase from which the keys are derived. • LINE – The passphrase (between 4 and 32 characters). • wep-defauly-key*<1-4>* – The key index used for transmission from the access port to MU.
wep64	Configure WEP64 parameters.

Example

```
RFS7000(config-wireless)#wlan 25 accounting syslog
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 answer-bcast-ess
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 authentication-type kerberos
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 description "TestWLAN"
RFS7000(config-wireless)#
```

```
RFS7000(config-wireless)#wlan 25 dot11i handshake timeout 2500 retransmit 5
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 dot11i key-rotation enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 dot11i key-rotation-interval 2000
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 hotspot webpage external failure "This feature
is under development"
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 kdc server primary 1.2.3.4 auth-port 50000
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 mobility enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 radius accounting timeout 30 retransmit 50
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 radius mobile-unit timeout 30 retransmit 5
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 ssid TestString
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 symbol-extensions fast-roaming enable
RFS7000(config-wireless)#

RFS7000(config-wireless)#wlan 25 syslog accounting server 12.13.14.125 port 5005
RFS7000(config-wireless)#
```

Appendix A Customer Support

Motorola's Enterprise Mobility Support Center

If you have a problem with your equipment, contact Enterprise Mobility support for your region. Contact information is available at: *http://www.symbol.com/contactsupport*.

When contacting Enterprise Mobility support, please provide the following information:

- Serial number of the unit
- Model number or product name
- Software type and version number

Motorola responds to calls by email, telephone or fax within the time limits set forth in support agreements. If you purchased your Enterprise Mobility business product from a Motorola business partner, contact that business partner for support.

Customer Support Web Site

Motorola's Support Central Web site, located at *www.symbol.com/support* provides information and online assistance including developer tools, software downloads, product manuals and online repair requests.

Downloads

http://symbol.com/downloads

Manuals

http://symbol.com/manuals

General Information

Obtain additional information by contacting Motorola at:

1-800-722-6234, inside North America
+1-516-738-5200, in/outside North America
http://www.motorola.com/

MOTOROLA INC.
1303 E. ALGONQUIN ROAD
SCHAUMBURG, IL 60196
http://www.motorola.com

72E-85984-01 Revision A
April 2007